แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

GUIDELINES FOR CYBER RESILIENCE DEVELOPMENT FRAMEWORK IN CLOUD COMPUTING

จิราพัชร์ พันธุ์ถาวรชัย

JIRAPAT PHANTAWORNCHAI

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

จิราพัชร์ พันธุ์ฉาวรชัย

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

GUIDELINES FOR CYBER RESILIENCE DEVELOPMENT FRAMEWORK IN CLOUD COMPUTING

JIRAPAT PHANTAWORNCHAI

A THEMATIC SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

SCHOOL OF INFORMATION TECHNOLOGY

SRIPATUM UNIVERSITY

2018

ชื่อหัวข้อสารนิพนธ์	แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ GUIDELINES FOR CYBER RESILIENCE DEVELOPMENT FRAMEWORK IN CLOUD COMPUTING
นักศึกษา	จิราพัชร์ พันธุ์ถาวรชัย รหัสประจำตัว 60501791
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ	เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อาจารย์ที่ปรึกษาสารนิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย
อาจารย์ที่ปรึกษาสารนิพนธ์ร่วม	ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะเทคโนโลยีสารสนเทศ
(ผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี)

วันที่.....เดือน.....พ.ศ. .....

คณะกรรมการการสอบสารนิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์)

..... กรรมการ
(ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.สุรศักดิ์ มังสิงห์)

สารนิพนธ์เรื่อง แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

คำสำคัญ ความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ การคืนสภาพได้ด้านไซเบอร์ การประมวลผลแบบคลาวด์

นักศึกษา จิราพัชร์ พันธุ์ถาวรชัย

อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย

อาจารย์ที่ปรึกษาร่วม ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง

หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะ เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

พ.ศ. 2561

บทคัดย่อ

การศึกษาวิจัยนี้ เพื่อเป็นแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ และพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ สำหรับกลุ่มตัวอย่างที่ใช้ในการดำเนินการวิจัยมีจำนวน 2 กลุ่ม คือ ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์จำนวน 6 ท่าน ในการสนทนากลุ่มและตอบข้อซักถามเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์เพื่อเป็นแนวทางในการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ และกลุ่มผู้ที่ทำงานเกี่ยวข้องกับระบบการประมวลผลแบบคลาวด์จำนวน 120 คนจาก 3 หน่วยงาน (TRUE, INET, UIH) เพื่อทำการประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ขององค์กรที่สังกัดอยู่

สรุปผลการทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์จะต้องพิจารณาด้านต่าง ๆ ดังนี้ 1) การระบุ (Identify) 2) การป้องกัน (Protect) 3) การตรวจจับ (Detect) 4) การตอบสนอง (Respond) 5) การคืนสภาพ (Recover) 6) . การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) โดยแต่ละด้านจะต้องสอดคล้องกับการดำเนินงานทางธุรกิจ เพื่อให้ระบบสามารถทำงานได้อย่างถูกต้อง และผลรวมการประเมินตนเองของหน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์จำนวน 3 หน่วยงาน อยู่ในระดับมาก ($\overline{X}$=3.53, S.D.=0.83) แสดงให้เห็นว่าผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ยังจำเป็นต้องพัฒนาทางด้านการระบุ, การตรวจจับ, และการสนับสนุนค้ำจุนให้ยั่งยืน

THEMATIC TITLE	GUIDELINES FOR CYBER RESILIENCE DEVELOPMENT FRAMEWORK IN CLOUD COMPUTING
KEYWORDS	INFORMATION SECURITY, CYBERSECURITY CYBER RESILIENCE, CLOUD COMPUTION
STUDENT	MR. JIRAPAT PHANTAWORNCHAI
ADVISOR	ASSIST. PROF. DR.NIVET CHIRAWIVHITCHAI
CO-ADVISOR	PROF. DR. PRASONG PRANEETPOLGRANG
LEVEL OF STUDY	MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
FACULTY	SCHOOL OF INFORMATION TECHNOLOGY SRIPATUM UNIVERSITY
YEAR	2018

ABSTRACT

This study This is a guideline for Cyber Resilience Development Framework in Cloud Computing. Develop and implement self-assessment applications for Cyber-reassessment for Cloud Computing. There were two groups of research samples, six Cybersecurity experts, in the group discussion and responses to Cybersecurity and Cyber Resilience questions. Cloud Computing as a Way to Build a Cyber Resilience Framework in Cloud Computing. There are 120 people working in the field of cloud computing, from (TRUE, INET, UIH), to self-assess for Cyber Resilience in Cloud Computing Affiliated organizations.

The results of the Cyber Resilience Development Framework in Cloud Computing. must take into account the following: 1) Identify 2) Protect 3) Detect 4) Respond 5) Recover 6) Sustain Each aspect of the business must be consistent with the business operation. For the system to work properly. And the self-assessment scores of the three cloud computing service providers were at a high level ($\overline{X}$=3.53, S.D.=0.83). Cloud computing also needs to develop identification, detection, and sustainability support.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้เกิดขึ้นและสำเร็จลุล่วงได้ เนื่องจากได้รับการสนับสนุนและ คำแนะนำเกี่ยวกับแนวทางในการศึกษาค้นคว้าข้อมูลและวิธีการปฏิบัติงาน จากอาจารย์ที่ปรึกษาศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง และ ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย อาจารย์ที่ปรึกษาสารนิพนธ์ เป็นอย่างดี จนสามารถทำวิจัยได้สำเร็จตามกรอบเวลาที่กำหนด ผู้จัดทำจึงขอขอบพระคุณเป็นอย่างสูงที่ได้เสียสละเวลาอันมีค่าในการให้คำปรึกษาและถ่ายทอดประสบการณ์ความรู้อันเป็นประโยชน์ต่อสารนิพนธ์ฉบับนี้

ผู้จัดทำขอขอบพระคุณคณาจารย์ทุกท่านที่ประสิทธิ์ประสาทวิชาความรู้ให้ ขอขอบพระคุณคุณพ่อ คุณแม่ และครอบครัว ที่ได้ให้กำลังใจด้วยดีตลอดมา รวมถึงผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ทั้ง 6 ท่านและผู้เกี่ยวข้องทางด้านความมั่นคงปลอดภัยไซเบอร์ของบริษัท TRUE INET และ UIH รวมถึงเพื่อน ๆ และเจ้าหน้าที่ของมหาวิทยาลัยศรีปทุมที่มีส่วนทำให้งานวิจัยนี้ประสบความสำเร็จด้วยดี และขอขอบพระคุณเจ้าของเอกสารและงานวิจัยทุกท่าน ที่ผู้จัดทำได้นำมาอ้างอิงในการทำวิจัยจนกระทั่งงานวิจัยฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี จึงขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

จิราพัชร์ พันธุ์ถาวรชัย

สารบัญ

บทที่ หน้า
บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VII
สารบัญภาพ VIII

1 บทนำ 1
ความเป็นมาและความสำคัญของปัญหา 1
วัตถุประสงค์ของการวิจัย 2
กรอบแนวคิดในการวิจัย 2
คำถามวิจัย 2
สมมติฐานการวิจัย 3
ขอบเขตของการวิจัย 3
ประโยชน์ที่คาดว่าจะได้รับ 3
นิยามศัพท์ 4

2 แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง 5
Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience 11
Cyber Resilience Best Practices 11
Cyber Security Resilience Complete Self-Assessment Guide 12
Cyber Resilience of Systems and Networks 13
ISO/IEC 27001 13
ISO/IEC 27002 15
ISO/IEC 27017 16

สารบัญ(ต่อ)

บทที่ หน้า

ISO/IEC 27018 17

งานวิจัยที่เกี่ยวข้อง 18

3 วิธีการดำเนินการวิจัย 19

ขั้นตอนการวิจัย 20

เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย 22

การกำหนดเกณฑ์พิจารณาระดับค่าคะแนน 23

สถิติที่ใช้ในการวิเคราะห์ข้อมูล 24

การวิเคราะห์ออกแบบระบบ 25

ระยะเวลาในการดำเนินงาน 27

สรุป 28

4 ผลการวิจัย 29

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1 29

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 2 30

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 3 34

5 สรุปผลการวิจัย 42

อภิปรายผล 47

ปัญหาและอุปสรรค 47

ข้อเสนอแนะ 48

บรรณานุกรม 49

ภาคผนวก ก คู่มือการใช้งานแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์ 55

สารบัญ(ต่อ)

บทที่ หน้า

ภาคผนวก ข แบบการสัมภาษณ์เชิงลึกความสามารถในการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 62

ภาคผนวก ค แบบประเมินตนเองการวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์ 66

ภาคผนวก ง ผลงานตีพิมพ์ 73

ประวัติผู้วิจัย 75

สารบัญตาราง

ตารางประกอบที่ **หน้า**

2.1 ตารางแสดง NIST Cybersecurity Framework V1.1 7

3.1 กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 21

3.2 ระยะเวลาในการดำเนินงาน 27

4.1 กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 31

4.2 ค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐานผลการประเมินประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์ของ หน่วยงานที่ 1 32

4.3 ค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐานผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์ของ หน่วยงานที่ 2 33

4.4 ค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐานผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์ของ หน่วยงานที่ 3 33

4.5 ค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐานผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์ สำหรับระบบการประมวลผลแบบคลาวด์โดยรวมของ 3 หน่วยงาน 34

5.1 กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 44

5.2 สรุปค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์ 44

สารบัญภาพ

ภาพประกอบที่ หน้า

1.1 กรอบแนวคิดในการวิจัย 2
2.1 Cybersecurity and Cyber Resilience Model (ISF)....8
2.2 PPT Concept (People Process and. Technology) 8
2.3 ACIS-Cybertron Cybersecurity Resilience Framework....9
2.4 CIA TRAID 15
3.1 Use Case Diagram แสดงความสัมพันธ์ของผู้ใช้งานระบบ....22
3.2 Software Development Life Cycle (SDLC) 25
3.3 วงจรโดยรวมของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 27
4.1 Use Case Diagram สำหรับแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 34
4.2 วงจรโดยรวมของการแนวทางการพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 35
4.3 ผังกระบวนการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 36
4.4 ฐานข้อมูลสำหรับแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 37
4.5 หน้าแรกของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 37
4.6 หน้าสำหรับเพิ่มหัวข้อในการประเมินตนเองสำหรับประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 38
4.7 หน้าสำหรับเพิ่มกลุ่มคำถามในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์....38
4.8 หน้าสำหรับเพิ่มคำถามในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์....39

4.9 หน้าสำหรับเพิ่มคำตอบในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์.....39
4.10 หน้าสำหรับเพิ่มชื่อบริษัทหรือองค์กรในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์.....40
4.11 หน้าสำหรับทำการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์.....40
4.12 หน้ารายงานผลการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์.....41
5.1 หน้าเข้าสู่ระบบของแอปพลิเคชันประเมินตนเอง.....45
5.2 หน้าเพิ่มชื่อบริษัทหรือองค์กร.....46
5.3 หน้าสำหรับทำการประเมิน.....46
5.4 หน้าสรุปผลการประเมิน.....47

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน บริษัทและองค์กรจำนวนมาก มีการเก็บข้อมูลสำคัญ ทั้งทางด้านการดำเนินงาน ข้อมูลลูกค้า และข้อมูลอื่น ๆ ที่มีความสำคัญเป็นจำนวนมาก ประกอบกับเทรนไอทีทางด้าน Cloud ที่เริ่มเข้ามามีบทบาทและเป็นที่นิยมใช้มากขึ้น ทำให้บริษัทและองค์กรต่าง ๆ เริ่มมีการใช้งานระบบการประมวลผลแบบคลาวด์หรือ Cloud Computing ทำให้รูปแบบการใช้งานและเข้าถึงข้อมูลมีความง่ายและสะดวกรวดเร็ว Cloud เป็น 1 ใน Mega Trend IT ที่กำลังเป็นที่นิยมมีทั้งหมด 4 ด้าน ได้แก่ Social (S) , Mobile (M) , Cloud (C) , Big Data (I) หรือ SMCI ซึ่งจากการนำเสนอของ บริษัทการ์ทเนอร์ จะพบว่าส่วนที่เกี่ยวข้องด้านความปลอดภัยไซเบอร์กับ SMCI มีทั้งหมด 2 ปัจจัยคือ 1. Privacy (ความเป็นส่วนตัว), 2. Security (ความปลอดภัย) การจะทำให้ระบบสามารถทำงานได้อย่างถูกต้องและต่อเนื่องจึงจำเป็นที่จะต้องมีมาตรการด้านความมั่นคงปลอดภัยไซเบอร์เข้ามาใช้ในการดำเนินงาน จากการวิจัยของ Information Security Forum (ISF) ระบุว่าระดับของความมั่นคงปลอดภัยไซเบอร์แบ่งได้เป็น 3 ระดับ คือ 1. Information Security, 2. Cybersecurity, 3. Cyber Resilience โดยแบ่งตามประเภทของการรับรู้ทางด้านความปลอดภัยคือ 1. Known CIA คือ การรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อ CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability การรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Information Security , 2. Known non-CIA คือ การรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อระบบอื่นนอกเหนือจาก CIA Triad การรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Cyber security , 3. Unknown คือ การรับมือกับภัยคุกคามที่ไม่เป็นที่รู้จัก หรือไม่เคยพบมาก่อนการรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Cyber Resilience การที่จะมีความมั่นคงปลอดภัยไซเบอร์ถึงระดับ Cyber Resilience จำเป็นที่จะต้องเริ่มจาก ระดับของ Information Security เสียก่อน

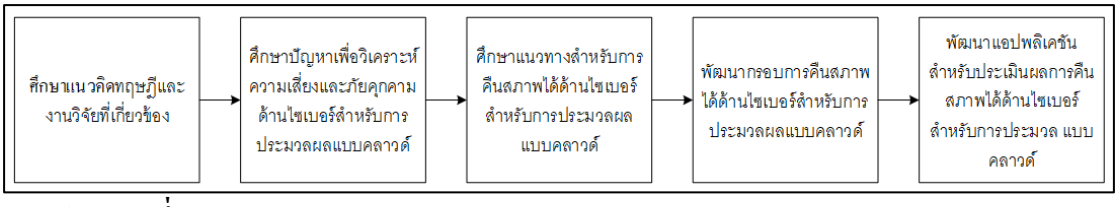
กล่าวโดยสรุปคือ การพัฒนาของเทคโนโลยี มีความรวดเร็วและสามารถเข้าถึงได้ง่ายมากขึ้นทำให้ ปัจจัยต่าง ๆ เอื้อต่อความไม่ปลอดภัยในการใช้งานทั้งในแง่ของ ความลับ ความถูกต้อง และความพร้อมใช้ ยิ่งมีการใช้งานและการเข้าถึงที่ง่ายมากขึ้นเท่าไหร่ ความเสี่ยงทางด้านความปลอดภัยก็ยิ่งมีมากขึ้น การมีมาตรการความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งที่จำเป็น และเข้า

มามีบทบาทในการดำเนินงาน ซึ่งความปลอดภัยที่เกิดขึ้นนั้นต้องคำนึงถึงภาพรวมของธุรกิจหรือกิจกรรมต่าง ๆ ที่มีผลกระทบ รวมถึงปัจจัยภายใน และภายนอก ที่อาจจะส่งผลต่อความมั่นคงปลอดภัยไซเบอร์ การจะพัฒนาระดับความปลอดภัยนั้นผู้บริหารมีความจำเป็นที่จะต้องเข้ามามีส่วนร่วมในการดำเนินงาน รวมถึงผลักดันให้เกิดการยอมรับในองค์กรณ์ ซึ่งจะเห็นได้ว่า กรอบทางด้านการคืนสภาพทางด้านไซเบอร์มีจุดเริ่มมากจาก กรอบการพัฒนาทางด้านความปลอดภัยไซเบอร์ ที่มีการนำมาจัดกลุ่มตามปัจจัยต่าง ๆ ที่มีผลกระทบต่อการดำเนินงาน รามถึงการรับมือทั้งก่อนและหลังเหตุการณ์ความผิดปกติที่เกิดขึ้น มาตรการรับมือต่าง ๆ ที่เกิดขึ้นมีเพียงจุดประสงค์เดียวคือการทำให้ระบบหรือธุรกิจสามารถให้บริการได้อย่างถูกต้องและต่อเนื่อง

วัตถุประสงค์ของการวิจัย

1. เพื่อวิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
2. เพื่อพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
3. เพื่อพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์

กรอบแนวคิดในการวิจัย



ภาพประกอบที่ 1.1 กรอบแนวคิดในการวิจัย

คำถามวิจัย

การคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ที่ดีควรเป็นอย่างไร และประกอบความสามารถของระบบในด้านใดบ้าง

สมมติฐานการวิจัย

แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ที่ดีควรคำนึงถึงปัจจัยต่าง ๆ ที่มีผลกระทบกับระบบหรือธุรกิจเพื่อให้ระบบหรือธุรกิจสามารถทำงานงได้อย่างถูกต้องและต่อเนื่อง

ขอบเขตของการวิจัย

ขอบเขตของงานวิจัยจะเป็นการศึกษาเรื่องความเสี่ยงและภัยคุกคามด้านไซเบอร์ และการคืนสภาพของระบบการประมวลผลแบบคลาวด์ (Could Computing) และพัฒนาแอปพลิเคชันสำหรับประเมินตนเองในการประเมินปัจจัยต่าง ๆ ที่มีผลต่อการคืนสภาพได้ของระบบการประมวลผลแบบคลาวด์ (Could Computing) โดยใช้ทฤษฎี NIST Cybersecurity Framework ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่ 1. การระบุ (Identify) 2. การตรวจจับ (Detect) 3. การป้องกัน (Protect) 4. การตอบสนอง (Respond) 5. การกู้คืน (Recover) มาพิจารณาควบคู่กับ Cybersecurity and Cyber Resilience Model และ การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) โดยกรอบงานหลัก 5 function ที่กล่าวมาจะถูกพิจารณาตามหัวข้อและเพิ่มข้อการสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) เพื่อให้คลอบคลุมในส่วนของการกำหนดนโยบายและการปฏิบัติ

1. ศึกษาความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
2. ศึกษาและพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
3. พัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ประโยชน์ที่คาดว่าจะได้รับ

1. ทราบถึง แนวทาง กระบวนการ และมาตรฐานการรักษาความมั่นคงปลอดภัย ไซเบอร์ของระบบการประมวลผลแบบคลาวด์
2. ทราบถึงระดับความพร้อมในการคืนสภาพของระบบการประมวลผลแบบคลาวด์
3. ทราบถึงปัญหาที่เกี่ยข้องกับการคืนสภาพของระบบการประมวลผลแบบคลาวด์
4. แอปพลิเคชันประเมินตนเองสำหรับการประเมินการคืนสภาพของระบบการประมวลผลแบบคลาวด์

นิยามศัพท์

Cloud Computing เป็นลักษณะการทำงานโดยใช้ทรัพยากรต่าง ๆ ที่มีอยู่มากมายบนเครือข่ายอินเทอร์เน็ต เช่น พื้นที่เก็บข้อมูล แพลตฟอร์มทางธุรกิจ แอปพลิเคชัน พาณิชย์อิเล็กทรอนิกส์ การตลาดออนไลน์ผู้ใช้งานคอมพิวเตอร์สามารถเลือกใช้งานได้ผ่านผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ที่ให้บริการใดบริการหนึ่งกับผู้ใช้ โดยผู้ให้บริการจะแบ่งปันทรัพยากร ให้กับผู้ต้องการใช้งานนั้น และจ่ายค่าบริการตามการใช้งานจริง

Information Security หมายถึง ระดับการรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อ CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability

Cyber Security หมายถึง ระดับการการรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อระบบอื่นนอกเหนือจาก CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability

Cyber Resilience หมายถึง คือ ระดับการคืนสภาพได้อย่างรวดเร็วสามารถรับมือกับภัยคุกคามที่ไม่เป็นที่รู้จัก หรือไม่เคยพบมาก่อนสามารถรับมือต่อการเปลี่ยนแปลง รวมทั้งความสามารถในการทนทานต่อการบุกรุก การโจมตี รวมถึงความสามารถในการคืนสภาพของระบบ ไม่ว่าจะเป็นการโจมตีที่เกิดจากปัจจัยภายในหรือภายนอก

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การวิจัยได้ดำเนินการทบทวนทฤษฎีแนวคิดและการวิจัยที่เกี่ยวข้องกับการวิเคราะห์และพัฒนาแอปพลิเคชันสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์เพื่อรวบรวมข้อมูลที่เป็นประโยชน์แก่การกำหนดแนวทางและวิธีการวิจัย โดยได้แบ่งออกเป็นหัวข้อ ดังนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 NIST Cybersecurity Framework V1.1

2.1.2 Cybersecurity and Cyber Resilience Model (ISF)

2.1.3 PPT Concept (People Process and Technology)

2.1.4 ACIS-Cybertron Cybersecurity Resilience Framework

2.1.5 Cyber Resiliency Engineering Framework (CREF)

2.1.6 Cyber Resiliency Design Principles, 2017

2.1.7 Advancing Cyber Resilience Principles and Tools for Boards

2.1.8 Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience

2.1.9 Cyber Resilience Best Practices

2.1.10 Cyber Security Resilience Complete Self-Assessment Guide

2.1.11 Cyber Resilience of System and Network

2.1.12 ISO/IEC 27001

2.1.13 ISO/IEC 27002

2.1.14 ISO/IEC 27017

2.1.15 ISO/IEC 27018

2.2 งานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 NIST Cybersecurity Framework V1.1

Framework Core Functions for Cyber security แบ่งย่อยออกเป็นกรอบงานหลัก 5 functions ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่

1. การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และ กิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

2. การป้องกัน (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสม สำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของ เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธี ปฏิบัติ ตลอดจนเทคโนโลยี

3. การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้าน ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตาม ต่อเนื่อง

4. การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อ เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

5. การคืนสภาพ (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับ การดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

การพัฒนากรอบของ NIST Cybersecurity Framework ได้อ้างอิงเนื้อหาบางส่วนจาก CCS CSC (Council on Cybersecurity: 20 Critical Security Control) , COBIT 5 (Govemance and Management of Enterprise IT) , ISA 62443-2-1:2009, an industrial automation and control systems (IACS) security management system , ISO/IEC 27001:2013 (Information Security Management System) , NIST SP 800-53 Rev.4 Security Control , http://www.nist.gov/cyberframwork เคยมีการจัดทำทั้งหมด 2 เวอร์ชั่น คือ เวอร์ชั่น 1.0 และ เวอร์ชั่น 1.1 ซึ่งแตกต่างกันที่ เวอร์ชั่น 1.1 มีการเพิ่ม Categories จาก 22 เป็น 23 ข้อ และ Subcategories จาก 98 เป็น 106 ข้อ นอกเหนือจากนั้นยังมีการ

ทบทวนสาระสำคัญจากปัจจัยการผลิต มีการระบุและพิจารณาประเด็นสำคัญหลายประการในระหว่างการอัพเดทคือ

1. เสริมสร้างการตรวจสอบและการจัดการข้อมูลใน Core Framework
2. เพิ่มคำแนะนำสำหรับความเสี่ยงในการซื้อและห่วงโซ่อุปทานการจัดการ (SCRM)
3. วิธีการวัดและสร้างตัวชี้วัดเพื่อความชัดเจนในระดับการดำเนินงานและความสัมพันธ์กิจกรรม โดยสามารถแสดง NIST Cybersecurity Framework V1.1 ดังตารางประกอบที่ 2.1

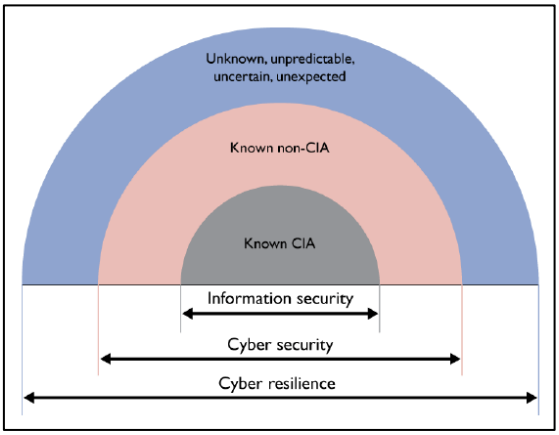
ตารางประกอบที่ 2.1 ตารางแสดง NIST Cybersecurity Framework V1.1

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

2.1.2 Cybersecurity and Cyber Resilience Model (ISF)

หน่วยงานอิสระ Information Security Forum (ISF) มุ่งเน้นการพัฒนามาตรฐาน เชิงเทคนิคทางด้านความมั่นคงปลอดภัยของข้อมูล ได้ทำการแบ่งภัยคุกคามและวิธีรับมือทางด้านความมั่นคงปลอดภัยไซเบอร์แบ่งได้เป็น 3 ระดับ คือ 1) Information Security , 2) Cybersecurity , 3) Cyber Resilience โดยแบ่งตามประเภทของการรับรู้ทางด้านความปลอดภัยคือ 1) Known CIA คือ การรับมือกับภัยคุกคามหรือความผิดปรกติที่เป็นที่รู้จักและส่งผลกระทบต่อ CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability การรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Information Security , 2) Known non-CIA คือ การรับมือกับภัยคุกคามหรือความผิดปรกติที่เป็นที่รู้จักและส่งผล

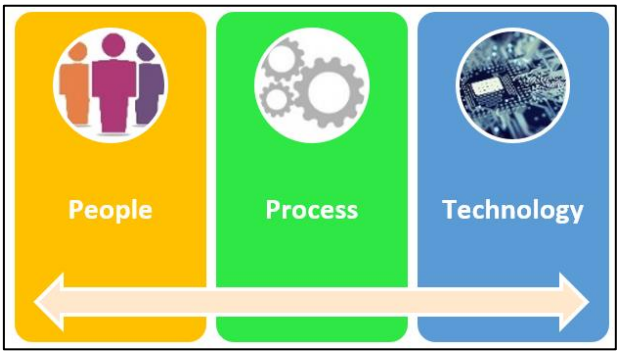
กระทบต่อระบบอื่นนอกเหนือจาก CIA Triad การรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Cyber security , 3) Unknown คือ การรับมือกับภัยคุกคามหรือความผิดปรกติที่ไม่เป็นที่รู้จัก ไม่คาดคิดหรือไม่เคยพบมาก่อนการรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Cyber Resilience ดังภาพประกอบที่ 2.1



ภาพประกอบที่ 2.1 Cybersecurity and Cyber Resilience Model (ISF)

2.1.3 PPT Concept (People Process and. Technology)

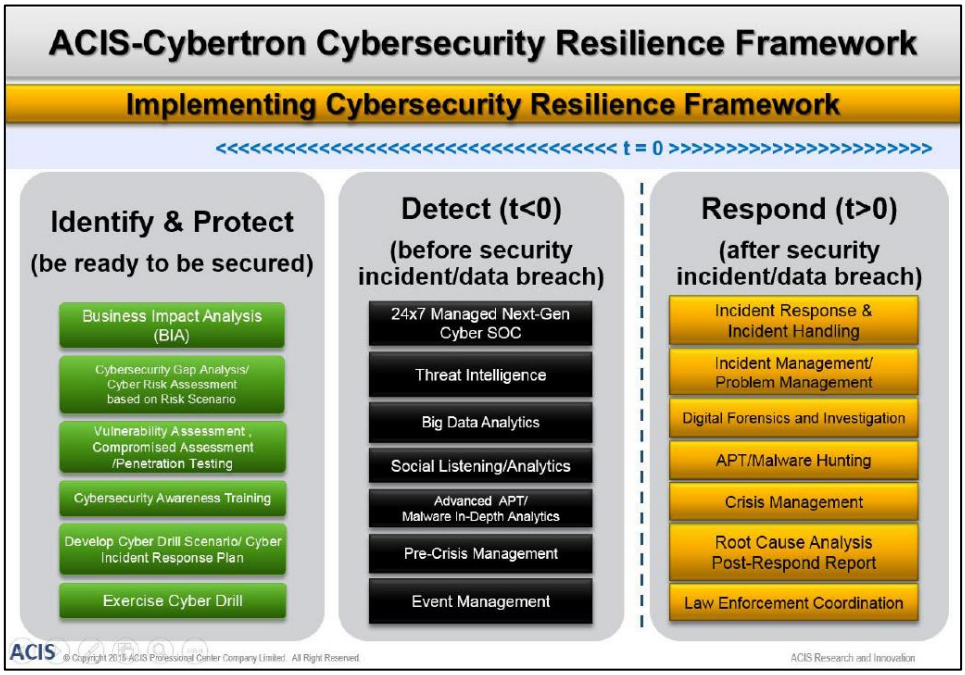
"PPT" หรือ "People", "Process" และ "Technology" ซึ่งเป็นแนวคิดในการบริหารจัดการเทคโนโลยีสารสนเทศ (IT Management) ตลอดจนการบริหารจัดการเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) โดยพยายามที่จะรักษาสมดุลระหว่าง เรื่องของกระบวนการ, เทคโนโลยี และ บุคลากร ผู้บริหารควรคำนึงถึงการปรับปรุงกระบวนการทำงานให้ได้มาตรฐานควบคู่ไปกับ การอบรมฝึกฝนบุคลากรในองค์กร ให้มีความรู้และมีความตระหนักในเรื่องความมั่นคงปลอดภัยสารสนเทศโดยไม่เน้นแต่การนำเทคโนโลยีมาใช้เพียงด้านเดียว ดังภาพประกอบที่ 2.2



ภาพประกอบที่ 2.2 PPT Concept (People Process and. Technology)

2.1.4 ACIS-Cybertron Cybersecurity Resilience Framework

ACIS-Cybertron ได้จัดทำ Cybersecurity Resilience Framework Implementation โดยใช้หลักการของ CsP-MICS (NexusFour) และ Cybersecurity Resilience Framework โดยแบ่งเป็น 3 หัวข้อใหญ่คือ 1. Identify & Protect (จัดทำเพื่อให้ระบบมีความพร้อมในด้านความปลอดภัย), 2. Detect (การรับมือก่อนที่เหตุการณ์ที่ไม่คาดคิดที่เกิดขึ้นกับระบบ), 3. Respond (การรับมือหลังจากเหตุการณ์ที่ไม่คาดคิดที่เกิดขึ้นกับระบบ) ดังภาพประกอบที่ 2.3



ภาพประกอบที่ 2.3 ACIS-Cybertron Cybersecurity Resilience Framework

2.1.5 Cyber Resiliency Engineering Framework (CREF)

MITRE Corporation ได้พัฒนา Cyber Resiliency Engineering Framework (CREF) ขึ้นในปี ค.ศ. 2011 โดยมีหลักการในการออกแบบหรือ Cyber Resiliency Design Principle อธิบายแนวคิดนี้ในปี ค.ศ. 2017 มุ่งเน้นไปที่ Advanced Cyber Threat หรือ Advanced Persistent Threat (APT) จึงจำเป็นต้องมีการออกแบบระบบให้มีความพิเศษในการรองรับการโจมตีในรูปแบบนี้ โดยเฉพาะ MITRE ได้นำหลักการในการออกแบบ 4 หัวข้อใหญ่มาใช้ ได้แก่ 1) Security 2) Resilience 3) Evolvability 4) Survivability ตัว CREF ได้รับการออกแบบมาโดยแบ่งออกเป็น 3 โดเมนหลัก ได้แก่ 1) Goals 2) Objectives 3) Techniques โดย Goals จะแบ่งออกเป็น 4 Goals ได้แก่ 1) Anticipate 2) Withstand 3) Recover 4) Evolve และแบ่ง Objective ออกเป็น 8 Objectives และ 14 Techniques โดย Technique จะสนับสนุน Objective CREF ได้ออกแบบมาให้เหมาะสมกับ Cyber Attack

Lifecycle ในปัจจุบัน Cyber Attack Lifecycle ได้รับการพัฒนาต่อยอดมาจาก Cyber Kill Chain โดยหลักการของ Cyber Resiliency จะเน้นเรื่องเวลาในการกู้คืนระบบ Time of Recovery การออกแบบจะคิดถึงความสัมพันธ์ ของ Cybersecurity และ Cyber Resilience โดย Cyber Resilience มุ่งเน้นไปที่ Mission Assurance และ Resilience/ Availability แต่ Cybersecurity มุ่งไปที่ Privacy และ Conventional Security

2.1.6 Cyber Resiliency Design Principles, 2017

Cyber Resiliency Design Principles, January 2017 ได้ให้คำจำกัดความของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง การป้องกันต่อความเสียหายรวมถึงการกู้คืนระบบคอมพิวเตอร์ ระบบการสื่อสารทางอิเล็กทรอนิกส์ การให้บริการสื่อสารทางอิเล็กทรอนิกส์ รวมถึงการปกป้องข้อมูลเพื่อให้อยู่ในสภาพพร้อมใช้ ความถูกต้องครบถ้วน การรักษาความลับ การพิสูจน์ตัวตน และการห้ามปฏิเสธความรับผิดชอบ MITRE สรุปหลักการพื้นฐานของ Cyber Resilience ได้เป็นรูปสามเหลี่ยม 4 รูป ทาง MITRE เองได้มองภาพในอนาคตว่า Cyber Resilience จะกลายเป็นส่วนหนึ่งของ Cybersecurity โดยการนำ Cyber Resilience Technique ต่าง ๆ มาใช้ เป็นไปตามหลักการของ Maturity ตั้งแต่ Immature ไปจนถึง Highly Mature ดัง กล่าวโดยสรุปจะเห็นว่า องค์กรทั่วโลกโดยเฉพาะองค์กรที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานที่มีความสำคัญยิ่งยวด (Critical Infrastructure) นั้น ควรให้ความสำคัญกับ 3 เรื่องใหญ่ ๆ ได้แก่ 1. Threat Models 2. Threat Information 3. Frameworks โดยเรื่องที่ 1 Threat Models จะเน้นไปที่ Cyber Attack Lifecycle หรือ Cyber Kill Chain ทำความเข้าใจกับภัยไซเบอร์ให้ถ่องแท้เสียก่อน จากนั้นหันมาดูเรื่องที่ 2 “Threat Information ” หมายถึง การติดตามข่าวสารภัยไซเบอร์ต่าง ๆ ติดตามเทคนิคใหม่ ๆ ของแฮกเกอร์ และ Zero Day Exploit ที่หลุดออกมาตลอดจนเรื่อง CTI (Cyber Threat Intelligence) รวมถึงเรื่องการแชร์ Threat Information ในรูปแบบการรวมตัวกันเป็น ISAC (Information Sharing and Analysis Center) และ ISAO (Information Sharing and Analysis Organizations) รวมทั้งการนำ NIST Cybersecurity Framework และ Cyber Resiliency Engineering Framework (CREF) มาใช้ในการบริหารจัดการปัญหาภัยไซเบอร์ที่นับวันจะมีความสลับซับซ้อนและรุนแรงขึ้นจะเห็นได้ว่าการบริหารจัดการกับภัยไซเบอร์ในปัจจุบันนิยมบริหารจัดการในลักษณะ Threat Orientated Approach ที่กำลังเป็นทิศทางของหลายองค์กรในโลกนี้ โดยมี Security Mindset ที่ว่า “ไม่มีระบบใดในโลกนี้ที่ปลอดภัย 100%” จึงต้องมีการนำหลักการ Cyber Resilience หรือ Cyber Resiliency เข้ามาใช้ในการเตรียมรับมือกับภัยไซเบอร์ของวันนี้และอนาคต

2.1.7 Advancing Cyber Resilience Principles and Tools for Boards

เครื่องมือที่รวมอยู่ใน Advancing Cyber Resilience Principles and Tools for Boards นี้มีไว้เพื่อช่วยผู้จัดทำยุทธศาสตร์ในระดับกรรมการและผู้บริหารระดับสูงเพื่อแนะนำการใช้ทรัพยากรด้านความปลอดภัยภายในองค์กรของตนเองอย่างมีประสิทธิภาพและเพื่อให้สามารถติดตามได้อย่างมีประสิทธิภาพและคล่องตัวตามเป้าหมายขององค์กรและให้ความรับผิดชอบสำหรับ cybersecurity และความยืดหยุ่นตลอดทั้งองค์กรเครื่องมือเหล่านี้ได้รับการยอมรับว่าความยืดหยุ่นเป็นจุดเน้นกลยุทธ์รวมถึงการดำเนินการขององค์กรก่อน,ระหว่างและหลังเหตุการณ์จึงยิ่งลดลงอย่างมากภัยคุกคามที่อาจเกิดขึ้น

2.1.8 Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience

ความคิดริเริ่ม Partnership for Cyber Resilience ที่เกี่ยวข้องกับองค์กรภาครัฐในการดำเนินงานพูดถึงบทบาทพิเศษที่รัฐบาลเข้ามาให้ทำให้สภาพแวดล้อมที่องค์กรดำเนินการลักษณะของเครือข่ายที่นำเสนอในโลกไซเบอร์ การกำหนดนโยบายที่มีความท้าทาย โดยเฉพาะอย่างยิ่งที่นั่นการตระหนักว่านโยบายที่ได้รับการออกแบบมาเพื่อเป็นทางออกกับปัญหาเฉพาะอย่างใดอย่างหนึ่งมักจะมีไม่ได้ตั้งใจผลที่อื่น ๆ เช่น เกี่ยวกับความเป็นส่วนตัวด้านนวัตกรรมหรือแม้กระทั่งธุรกิจที่มีอยู่และเป็นที่ยอมรับโดยทั่วไปในการปฏิบัติงาน

2.1.9 Cyber Resilience Best Practices

กลยุทธ์ด้านความยืดหยุ่นทางไซเบอร์ช่วยให้กิจกรรมต่าง ๆ ที่ดำเนินการเพื่อปกป้องค์กร สินทรัพย์และข้อมูลสอดคล้องกัน ทำให้แน่ใจได้ว่าเป้าหมายด้านความยืดหยุ่นของไซเบอร์มีสอดคล้องกับความต้องการของผู้มีส่วนได้เสีย การพัฒนากลยุทธ์ควรดำเนินการโดยผู้บริหารเป็นส่วนสำคัญของระบบการจัดการ กลยุทธ์เป็นมากกว่าแผน นอกจากนี้ยังมีกรอบการทำงานที่องค์กรสามารถปรับให้เข้ากับสภาพแวดล้อมที่เปลี่ยนแปลงได้ ซึ่งเหมาะสมกับการตอบสนองต่อภัยคุกคามที่ไม่รู้จักก่อนและช่องโหว่สามารถทำได้ในลักษณะที่ สอดคล้องกับเป้าหมายและเจตนารมณ์ขององค์กร หากปราศจากยุทธศาสตร์กิจกรรมความยืดหยุ่นในโลกไซเบอร์อาจไม่ปะติดปะต่อกัน

การออกแบบความยืดหยุ่นของความมั่นคงปลอดภัยไซเบอร์ (service design) เมื่อกำหนดกลยุทธ์ไว้ขั้นตอนต่อไปคือการออกแบบทุกสิ่งทุกอย่างที่จำเป็น เปลี่ยนกลยุทธ์ให้เป็นความจริง ออกแบบที่ดีจะเป็นรากฐานที่มั่นคงเพื่อให้แน่ใจได้ว่ากระบวนการและการควบคุมสามารถใช้งานได้ในภายหลังและเป็นไปตามความจำเป็นขององค์กร สามารถเปลี่ยนสภาพแวดล้อมการดำเนินงานได้อย่างมีประสิทธิภาพหากความยืดหยุ่นในโลกไซเบอร์ไม่ได้รับการออกแบบ การควบคุมความปลอดภัยจะมีการพัฒนาไปในแบบเฉพาะกิจ การออกแบบที่ดียังสามารถช่วยป้องกันการทำซ้ำของกระบวนการ

การเปลี่ยนผ่านการบริการ (service transition) การเปลี่ยนผ่านคือขั้นตอนของวงจรซึ่งการออกแบบจะนำไปสู่การปฏิบัติงาน องค์กรที่ไม่มีอะไรเปลี่ยนแปลงจะไม่สามารถรับมือกับความเสี่ยงใหม่ ๆ และไม่สามารถที่จะอยู่รอดได้ในระยะยาว เมื่อใดก็ตามที่มีการเปลี่ยนแปลงมีความเสี่ยงที่จะเกิดช่องโหว่ของระบบ การเปลี่ยนแปลงนี้รวมถึงการเปลี่ยนแปลงบุคคลที่รับผิดชอบ กระบวนการและเทคโนโลยี วัตถุประสงค์หลักของขั้นตอนการเปลี่ยนแปลงของวงจรคือการจัดการความเสี่ยงเหล่านี้เพื่อความความคล่องตัวโดยไม่กระทบต่อความต้องการทางธุรกิจ

การดำเนินการบริการอย่างต่อเนื่อง (Cyber Resilience Cyber resilience operation and continual) การทำงานที่ยืดหยุ่นของการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของวงจรที่มีการควบคุมทำ ให้กลยุทธ์ และการออกแบบ สามารถทำงานได้อย่างต่อเนื่อง จำเป็นต้องมีการตรวจสอบการทำงาน และฝึกซ้อมเพื่อให้พร้อมรับมือกับเหตุการณ์ที่ไม่คาดคิด

การปรับปรุงการให้บริการ (Cyber resilience improvement) การปรับปรุงอย่างต่อเนื่องไม่ใช่แค่เรื่องที่กำลังดำเนินการอยู่เท่านั้น ทุกอย่างที่องค์กรทำควรอยู่ภายใต้กระบวนการของความเข้าใจและการปรับปรุง ในทำนองเดียวกันองค์กรควรปรับปรุงกลยุทธ์อย่างต่อเนื่องให้ทันต่อยุคสมัยและเทคโนโลยี รวมถึงความสามารถในการเรียนรู้และปรับปรุงเพื่อหลีกเลี่ยงการทำผิดพลาดเดียวกันซ้ำแล้วซ้ำอีก มีการตรวจสอบเพื่อยืนยันถึงผลที่เกิดขึ้นหลังการปรับปรุง

2.1.10 Cyber Security Resilience Complete Self-Assessment Guide

การประเมินตนเองของ Cyber Security Resilience Complete Self-Assessment Guide ได้รับการพัฒนาเพื่อปรับปรุงความเข้าใจในข้อกำหนดและองค์ประกอบของไซเบอร์ และความยืดหยุ่นในการรักษาความปลอดภัยโดยอ้างอิงจากแนวทางและมาตรฐานที่ดีที่สุดมาประกอบกับกระบวนการทางธุรกิจการออกแบบและการจัดการคุณภาพ การประเมินตนเองนี้ออกแบบมาเพื่อให้สามารถประเมินตนเองได้อย่างรวดเร็ว เพื่อพิจารณาว่ามีความพร้อมมากน้อยเพียงใด เป็นประโยชน์ในการปรับปรุงประสิทธิภาพโดยรวมขององค์กรโดยแบ่งเป็นทั้งหมด 7 ด้านคือ 1.ความตระหนักรู้

(Recognize) 2.การกำหนด (Define) 3. มาตรการ (Measure) 4.การวิเคราะห์ (Analyze) 5.การปรับปรุง (Improve) 6.การควบคุม (Control) 7.การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain)

2.1.11 Cyber Resilience of Systems and Networks

การเพิ่มประสิทธิภาพของระบบและระบบเครือข่ายทางด้านความยืดหยุ่นไซเบอร์ แบ่งออกเป็น 4 บทคือ 1) การพิจารณาความยืดหยุ่นของไซเบอร์ในเชิงปริมาณ (Quantifying Cyber Resilience) การเก็บรวบรวมข้อมูลและเหตุการต่าง ๆ ที่เกิดขึ้นกับระบบมาวิเคราะห์ในเชิงปริมาณเช่น ข้อมูลการรับข้อมูลเข้าและออกต่อวัน ต่อเดือน และต่อปีของ Web Server เพื่อนำมาวิเคราะห์อัตราการเพิ่มขึ้นของปริมาณการรับส่งข้อมูลต่อปี และนำข้อมูลมาวางแผนในการเพิ่มประสิทธิภาพของ Web Server การพิจารณาคุณลักษณะต่าง ๆ ที่เกี่ยวข้องกับความยืดหยุ่นไซเบอร์ในเชิงปริมาณมีความสำคัญเพื่อนำมาเพิ่มประสิทธิภาพของความยืดหยุ่นไซเบอร์ 2) การประเมินและวิเคราะห์ความยืดหยุ่นของไซเบอร์ (Assessment and Analysis of Cyber Resilience) องค์กรส่วนมากยังให้ความสำคัญกับความยืดหยุ่นของระบบน้อยทำให้แนวทางในการปฏิบัติยังไม่ดีเท่าที่ควรวัตถุประสงค์ในบทนี้คือการร่างแนวทางปฏิบัติที่ดีที่สุดในหลาย ๆ ด้านที่เกี่ยวข้องกับความยืดหยุ่นในโลกไซเบอร์เพื่อให้สามารถเลือกนำไปประยุกต์ใช้กับระบบงานเช่น The National Institute of Standards and Technology's (NIST) Framework 3) การเพิ่มประสิทธิภาพความยืดหยุ่นไซเบอร์ (Enhancing Cyber Resilience) การเพิ่มประสิทธิภาพความยืดหยุ่นไซเบอร์ต้องเริ่มจากพื้นฐาน การพิจรณากระบวนการทางด้านความยืดหยุ่น และการนำเทคโนโลยีมาปรับใช้เพื่อเพิ่มความยืดหยุ่นไซเบอร์ การใช้งานการรักษาความปลอดภัยในโลกไซเบอร์ที่มีประสิทธิภาพ การปฏิบัติเหล่านี้มักเกี่ยวข้องกับการใช้ NIST Cybersecurity Framework และการดำเนินการปฏิบัติอย่างต่อเนื่อง 4) กรณีศึกษาความยืดหยุ่นของระบบและระบบเครือข่าย (Cyber Resilience in Selected Classes of Systems and Networks) กรณีศึกษาความยืดหยุ่นของระบบและระบบเครือข่ายเพื่อทำความเข้าใจกับประเภทของภัยคุกคามและช่องโหว่ของโครงสร้างพื้นฐานที่สำคัญ รวมถึง ความสำคัญของการเลือกที่ตั้ง การรับมือกับภัยธรรมชาติ การก่อการร้าย การโจมตีทางไซเบอร์ นำมาวิเคราะห์เพื่อหาแนวทางการรับมือกับผลกระทบที่เกิดขึ้น

2.1.12 ISO/IEC 27001

เป็นมาตรฐานที่เกี่ยวกับการบริหารจัดการข้อมูลสารสนเทศให้มั่นคงปลอดภัย การจัดทำระบบบริหารจัดการ (Management System) จะต้องพิจารณาหลายด้านที่มีความเกี่ยวข้อง

1.การบริหารคน

2.กระบวนการและเทคโนโลยี (เข้าใจกระบวนการทำงาน และเทคโนโลยีที่เหมาะสมในการนำมาใช้งาน)

3.บริหารงบประมาณ

มาตรฐานนี้ได้ถูกจัดทำขึ้นโดยยึดตามแนวคิดของหลักการ PDCA เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบ และมีการพัฒนาขึ้นอย่างต่อเนื่อง เริ่มต้นตั้งแต่การจัดตั้ง (Establish) การนำระบบไปใช้ (Implement) การดำเนินงาน (Operate)การติดตามและวัดผล (Monitor) การทบทวน (Review) การบำรุงรักษาระบบ (Maintain) และการปรับปรุงพัฒนาระบบให้ดียิ่งขึ้น (Improve)

การนำมาตรฐาน ISO27001 มาใช้งาน มี 4 องค์ประกอบใหญ่คือ

1.จัดทำระบบ(Establish)การจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System -ISMS) คือ การเตรียมการ วางแผนเพื่อปกป้องสารสนเทศ

2.นำไปปฏิบัติ(Implement) คือ นำแผนจากขั้นตอนการจัดทำระบบ(Establish)ไปปฏิบัติจริงหน้างาน ทำตามเอกสารคู่มือและลงบันทึกในแบบฟอร์ม

3.รักษาไว้(Maintain) คือปฏิบัติควบคู่ไปกับการทำงานปกติ

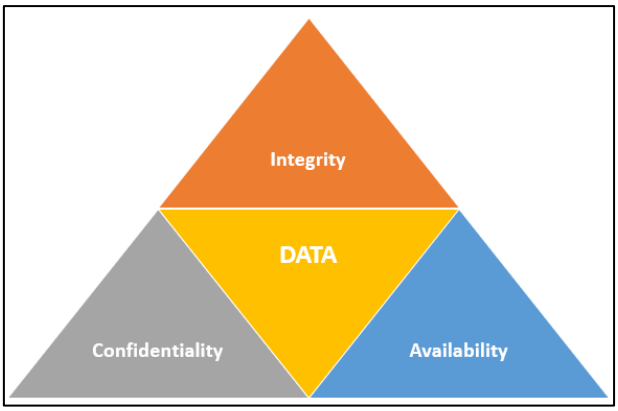
4.ปรับปรุงอย่างต่อเนื่อง(Continual Improvement) คือ ทบทวนผลการทำระบบและหาจุดปรับปรุงอย่างต่อเนื่อง ไม่ใช่ทำครั้งเดียวจบ

โมเดล CIA ใน ISO27001 เน้นการปกป้องข้อมูลสารสนเทศ (Information) ให้มีคุณสมบัติ 3ประการ ดังภาพประกอบที่ 2-5 โดยสรุปคือ

1.Confidential : การปกป้องสารสนเทศให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ ถ้าหากข้อมูลรั่วไหลแสดงว่าขาดคุณสมบัติในข้อนี้

2.Integrity : ปกป้องความถูกต้องสมบูรณ์ของสารสนเทศไม่ให้ถูกแก้ไขเปลี่ยนแปลงผิดไปจากความเป็นจริง เช่น การแฮกระบบเพื่อแก้ไขข้อมูล เป็นต้น

3.Availability : สร้างความเชื่อมั่นว่าระบบสารสนเทศพร้อมใช้งาน ดังภาพประกอบที่ 2.4



ภาพประกอบที่ 2.4 CIA TRAID

2.1.13 ISO/IEC 27002

ISO/IEC 27002:2005 เป็นชื่อใหม่ของ ISO 17799 ซึ่งเดิมใช้ชื่อว่า "BS 7799 Part 1" เป็นมาตรฐานแสดง หลักการปฏิบัติสำหรับ Information Security Management ที่อธิบายวัตถุประสงค์ของระเบียบวิธีการควบคุมด้าน Information Security ทั้งหลายอย่างละเอียด และแสดงวิธีปฏิบัติที่ดีที่สุด ของการควบคุมความมั่นคงปลอดภัย ISO/IEC 27002:2005 มีเนื้อหากล่าวถึงข้อควรปฏิบัติในการควบคุมความมั่นคงของข้อมูลที่องค์กรควรนำไปใช้ ซึ่งจะมีทั้งหมด 133 หัวข้อ และแบ่งออกเป็น 11 หัวข้อหลัก โดยจะมีการให้แนวทางในการปฏิบัติ (Implementation Guide) สำหรับแต่ละหัวข้อด้วย

หัวข้อสำคัญ 11 หัวข้อใหญ่ ในมาตรฐาน 27002:2005 มีดังต่อไปนี้

1. นโยบายเรื่องความมั่นคงปลอดภัย (Security policy) ประกอบด้วยนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์เพื่อกำหนดและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ เพื่อให้สอดคล้องกับข้อกำหนดทางธุรกิจ ระเบียบ และกฎหมายที่เกี่ยวข้อง โดยผู้บริหารต้องมีการจัดทำนโยบายเป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนด โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร โดยได้ระบุถึงบทบาทหน้าที่ของผู้บริหาร

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร ได้ระบุถึงบทบาทหน้าที่ของผู้บริหาร

3. การบริหารจัดการทรัพย์สินขององค์กร ได้กล่าวถึงบทบาทของหัวหน้างานทางด้านระบบสารสนเทศ และหัวหน้างานทางด้านพัสดุในแง่มุมต่าง ๆ

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคล โดยได้ระบบทบาทของผู้บริหาร หัวหน้างานระบบสารสนเทศ หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง

5.การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและทางด้านสิ่งแวดล้อม โดยได้กล่าวถึงบทบาทหน้าที่ของหัวหน้างานระบบสารสนเทศและหัวหน้างานอาคารในด้านต่าง ๆ

6.การบริหารจัดการด้านการสื่อสารและการดำเนินงานเครือข่ายระบบสารสนเทศขององค์กร โดย ได้ระบุถึงบทบาทของผู้บริหาร หัวหน้างานสารสนเทศ ผู้เป็นเจ้าของกระบวนการธุรกิจและพนักงานสารสนเทศในด้านต่าง ๆ

7.การควบคุมการเข้าถึง โดยได้ระบุถึงบทบาทของผู้บริหาร หัวหน้างานสารสนเทศ ผู้ดูแลระบบและพนักงานในด้านต่าง ๆ

8.การจัดหาการพัฒนาและการบำรุงรักษาระบบสารสนเทศ โดยได้ระบุถึงบทบาทของหัวหน้างานสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่าง ๆ

9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยได้ระบุถึงบทบาทของหัวหน้างานสารสนเทศ หัวหน้างานนิติกร ผู้ดูแลระบบและพนักงานในด้านต่าง ๆ

10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร โดยได้ระบุถึงบทบาทของผู้บริหาร และหัวหน้างานสารสนเทศ ที่เกี่ยวกับหัวข้อพื้นฐานการบริหารความต่อเนื่องในการดำเนินงาน เพื่อป้องกันการการหยุดชะงักของกิจกรรมต่าง ๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญเป็นผลมาจากการล้มเหลว ที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับมาได้ภายในระยะเวลาที่เหมาะสม

11.การปฏิบัติตามข้อกำหนด โดยได้ระบุถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานนิติกร ในด้านต่าง ๆ

2.1.14 ISO/IEC 27017

เป็นข้อมูลแนวทางปฏิบัติ ในการจัดการความปลอดภัยของการให้บริการคลาวด์ ซึ่งเป็นส่วนเสริมเพิ่มเติมจาก ISO 27002 โดยมีการเพิ่ม Cloud Computing Service Set เพื่อสร้างและรักษาความสัมพันธ์ในการทำงานร่วมกันระหว่างผู้ใช้บริการคลาวด์และผู้ให้บริการคลาวด์ในเรื่องการจัดการความปลอดภัยของข้อมูล

1. มีการควบคุมการเข้าถึงข้อมูลของลูกค้าบริการคลาวด์ใน Virtual Environment ที่ใช้ร่วมกัน ผู้ใช้บริการต้องได้รับความคุ้มครองและแบ่งแยกอย่างชัดเจนจากผู้ใช้บริการรายอื่น ๆ และจากผู้ซึ่งไม่ได้รับอนุญาตให้เข้าถึง

2. Operation Logs และ Logs การเข้าสู่ระบบบริการคลาวด์ ต้องมีระบบการจัดการที่ถูกต้องเหมาะสม สามารถเรียกดูได้และเก็บรักษาไว้อย่างถูกต้องปลอดภัย

3. ในด้านของความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลบนคลาวด์

3.1 มีระบบจัดการ Information Security Incident และตอบสนองต่อผู้ใช้บริการอย่างเหมาะสม

3.2 มีข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการกับผู้รับบริการ (SLA) ที่เหมาะสมในเรื่องของการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลที่เก็บไว้ในระบบของผู้ให้บริการ

2.1.15 ISO/IEC 27018

เป็นข้อมูลแนวทางปฏิบัติ สำหรับการปกป้องรักษาข้อมูลสำหรับการให้บริการคลาวด์สารณะ (Public Cloud) ในเรื่องของการปกป้องข้อมูล (Data Protection) โดยมีการกล่าวถึง Personal Identifiable Information (PII) ซึ่งหมายถึง ข้อมูลส่วนบุคคลต่าง ๆ ที่สามารถเชื่อมโยงถึงบุคคลใดบุลคลหนึ่งได้ เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือ อีเมล์ เป็นต้น ผู้ให้บริการ Public Cloud ถือเป็น PII Processors หมายถึง ผู้ทำหน้าที่ดำเนินการประมวลผลข้อมูลส่วนบุคคล (PII) ในนามของ PII Controller หรือปฏิบัติตามคำแนะนำของ PII Controller

PII Controller มีหน้าที่รับผิดชอบในการเก็บรวบรวม ควบคุมการใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยต้องจัดทำนโยบายการปกป้องข้อมูลส่วนบุคคล เช่น ข้อมูลอะไรบ้างที่มีการเก็บรวบรวม ใช้ข้อมูลของผู้ใช้งานอย่างไร เพื่ออะไร ส่งต่อข้อมูลของผู้ใช้งานกับใครบ้าง เจ้าของข้อมูลจะสามารถควบคุมและเข้าถึงข้อมูลของตนเองได้อย่างไร และมีการปกป้องข้อมูลอย่างไรเจ้าของข้อมูลต้องมีการยืนยันการรับรู้เกี่ยวกับการรวบรวมข้อมูลและการใช้งานข้อมูลดังกล่าวข้างต้น เจ้าของข้อมูลมีสิทธิ์ที่จะบอกรับ ยกเลิกและร้องเรียนหากมีการละเมิดสิทธิ์ เป็นต้น

2.2 งานวิจัยที่เกี่ยวข้อง

เอกฉัตร บ่ายคล้อย (2560) วิจัยเรื่อง การพัฒนาตัวแบบวุฒิภาวะความสามารถการรักษาความมั่นคงปลอดภัยสารสนเทศในระบบบริการแบบคลาวด์ เพื่อรองรับการคืนสภาพได้ ทางด้านการประมวลผลแบบคลาวด์ พบว่า ข้อมูลที่ถูกโจมตี ส่วนใหญ่เกิดขึ้นเมื่อข้อมูลอยู่ในฝั่งของผู้ให้บริการ คลาวด์ โดยการปล่อยมัลแวร์เข้าสู่ระบบ เป็นการโจมตีที่พบมากที่สุด การที่มีข้อมูลมารวมตัวกันมาก ๆ หากถูกโจมตีสำเร็จ ย่อมต้องมีการสูญเสียมหาศาล ดังนั้นจึงเป็นเหตุจูงใจที่ทำให้เกิดการ จากการศึกษาครั้งนี้สามารถชี้ให้เห็นชัดว่า ในการทำการศึกษาในอนาคตควรเน้นที่จะศึกษาเพิ่มเติมรวมทั้งหาทางป้องกันและแก้ไขเหตุการณ์ ในส่วนของข้อมูลที่จะถูกโจมตีในฝั่งของ ผู้ให้บริการ เป็นสำคัญ

วิภารัตน์ ปทักขินัง และ ประสงค์ ปราณีตพลกรัง (2557) วิจัยเรื่อง การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อม ด้านความมั่นคงปลอดภัยทางไซ

เบอร์ ขององค์กร พบว่า ส่วนประกอบของความพร้อมทางด้านความมั่นคงปลอดภัยทางไซเบอร์ จะประกอบไปด้วย 7 ด้าน คือ 1. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ 2. กฎระเบียบที่เกี่ยวข้อง 3. ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ 4. การป้องกันอาญากรรมไซเบอร์ 5. การพัฒนากำลังพลด้านไซเบอร์ 6. งบประมาณการวิจัย 7. ความร่วมมือกับหน่วยงานอื่น ๆ สำหรับตัวแบบประเมินความเสี่ยงจะประกอบไปด้วย 4 ด้าน ได้แก่ 1. กำหนดหัวข้อการบริหารจัดการความเสี่ยง 2. การวิเคราะห์ความเสี่ยง 3. การวางแผนการลดความเสี่ยง และ 4. การรายงานและการประเมินผล

ศิวลีย์ สิริโรจน์บริรักษ์ (2558) วิจัยเรื่อง การพัฒนามาตรฐาน การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม พบว่า “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม” มีจุดประสงค์เพื่อศึกษานโยบายและมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล และเพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานระดับสากล

เศรษฐพงค์ มะลิสุวรรณ (2558) วิจัยเรื่อง National Cybersecurity Strategy (ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ) พบว่า การสร้างความมั่นคงปลอดภัยไซเบอร์ไม่ใช่เพียงแค่วิสัยทัศน์อีกต่อไปเพราะหากไม่ลงมือสร้างขีดความสามารถทางด้านบุคลากรและเครื่องมือทางเทคโนโลยี ประเทศไทยก็จะประสบกับหายนะที่รับไม่ได้ในอนาคตอย่าง เพราะภัยคุกคามทางไซเบอร์เริ่มปรากฏชัด ดังนั้น ประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการบัญญัติกฎหมายที่เกี่ยวข้องในการเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ และจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างเร่งด่วน เพื่อ ให้ทันต่อการเติบโตของภัยคุกคามด้านไซเบอร์

Nazli Choucri และ Stuart Madnick และ Priscilla Koepke (2559) วิจัยเรื่อง Institutions for Cyber Security: International Responses and Data Sharing Initiatives พบว่าจากการขยายตัวของไซเบอร์สเปซเกิดขึ้นอย่างรวดเร็วในช่วง 2 ทศวรรษที่ผ่านมา แทบทุกสถานที่ตั้งในโลกนี้มีระดับการเข้าถึงไซเบอร์สูงกว่าที่คาดการณ์ไว้ การตั้งทฤษฎีเกี่ยวกับ Cyberpolitics ในความสัมพันธ์ระหว่างประเทศ จุดประสงค์คือการเริ่มต้นติดตามการตอบสนองของสถาบันที่เกี่ยวข้องต่อการเปลี่ยนแปลงอย่างรวดเร็ว 1. การสำรวจสำมะโนประชากรเพื่อให้ทราบถึงการคงอยู่ของบุคคลต่าง ๆ 2. ให้ข้อมูลที่มีความสำคัญและส่งผลต่อการพัฒนาของกระบวนการ 3. การกำหนดนโยบายภัยคุกคามทางไซเบอร์และอาชญากรรมไซเบอร์ระหว่างประเทศและระดับชาติ 4. สร้างกลไกลใหม่เพื่อตอบสนองต่อภัยคุกคามในโลกไซเบอร์

บทที่ 3
วิธีการดำเนินการวิจัย

การวิจัยเรื่องแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีวัตถุประสงค์ (1) เพื่อวิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ (2) เพื่อพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ (3) เพื่อพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ โดยเนื้อหาในบทนี้ผู้วิจัยกล่าวถึงประเด็นหลัก ดังนี้

3.1 ขั้นตอนการวิจัย

3.2 เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย

3.3 การกำหนดเกณฑ์พิจารณาระดับค่าคะแนน

3.4 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

3.5 การวิเคราะห์ออกแบบบระบบ

3.6 ระยะเวลาในการดำเนินงาน

3.7 สรุป

งานวิจัยนี้ได้ออกแบบมาเพื่อค้นหาคำตอบของคำถามวิจัยตามที่สร้างไว้ในบทที่ 1 ผู้วิจัยเริ่มต้นจากการหาข้อมูที่เกี่ยวข้องกับ Information Security , Cybersecurity และ Cyber Resilience รวมถึงการใช้งานระบบ Cloud หลังงจากนั้นจึงนำข้อมูลที่ได้วิเคราะห์ถึงความเสี่ยงและมั่นคงปลอดภัยสารสนเทศในระบบบริการแบบคลาวด์ หลังจากนั้น จึงทำการออกแบบกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์โดยอ้างอิงแนวคิดพื้นฐานจากตัวแบบ NIST Cybersecurity Framework เพื่อให้เห็นถึงวิธีการที่จะยืนยันว่าผลการประเมินตนเองที่ได้จากกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ความสอดคล้องกับการรับรู้ของผู้ให้บริการคลาวด์ งานวิจัยนี้จึงออกแบบให้มีวัตถุประสงค์หลัก 3 ข้อ ดังที่กล่าวถึงในตอนต้น พร้อมตั้งสมมติฐานในการดำเนินงานวิจัย ได้แก่ ระดับความสามารถการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์มีอยู่ในระดับปานกลางดังนั้นเพื่อให้สามารถดำเนินงานได้ตามวัตถุประสงค์หลัก และสามารถตอบสมมติฐานของการวิจัยตามที่กำหนดไว้ได้ ผู้วิจัยจึงได้กำหนดขอบเขตการดำเนินงานวิจัยเป็น 3 ส่วนหลัก ดังนี้ 1) การดำเนินการศึกษาเพื่อพัฒนากรอบที่ใช้ในการประเมินความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 2) ทำการ

พัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ และ 3) การดำเนินการพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ อย่างไรก็ดี สำหรับวิธีการดำเนินงานวิจัยจะถูกนำเสนออย่างเป็นลำดับตามที่กำหนดไว้ ในหัวข้อถัดไป

3.1 ขั้นตอนการวิจัย

ผู้วิจัยได้แบ่งขั้นตอนการวิจัยออกเป็น 3 ขั้นตอนหลัก โดยยึดตามลำดับของวัตถุประสงค์ในการวิจัย โดยมีรายละเอียดเนื้อหาดังต่อไปนี้

3.1.1 ขั้นตอนที่ 1 : เพื่อให้บรรลุตามวัตถุประสงค์ข้อที่ 1

ผู้วิจัยได้ทำการศึกษา สำรวจ ตรวจสอบ แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องดังที่ได้นำเสนอในบทที่ 2 และสัมภาษณ์ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์นั้นจะอิงตามแนวคิดมาตรฐาน และตัวแบบที่เกี่ยวข้อง ได้แก่ NIST Cybersecurity Framework, ACIS-Cybertron Cybersecurity Resilience Framework, Cyber Resilience Best Practices, Cyber Security Resilience Complete Self-Assessment Guide และ Cyber Resilience of Systems and Networks การดำเนินงานในขั้นตอนนี้เป็นไปเพื่อวิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์และหาแนวทางในการพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

3.1.2 ขั้นตอนที่ 2 : เพื่อให้บรรลุตามวัตถุประสงค์ข้อที่ 2

ผู้วิจัยได้ดำเนินการพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ และจัดทำแบบประเมินตนเองเรื่องผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ เพื่อรวบรวมข้อมูลมาทำการประเมิน โดยแยกหัวข้อในการประเมินตนเองเป็น การระบุ (Identify), การตรวจจับ (Detect), การป้องกัน (Protect), การตอบสนอง (Respond), การคืนสภาพ (Recover) และการสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ดังตารางประกอบที่ 3.1

ตารางประกอบที่ 3.1 กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

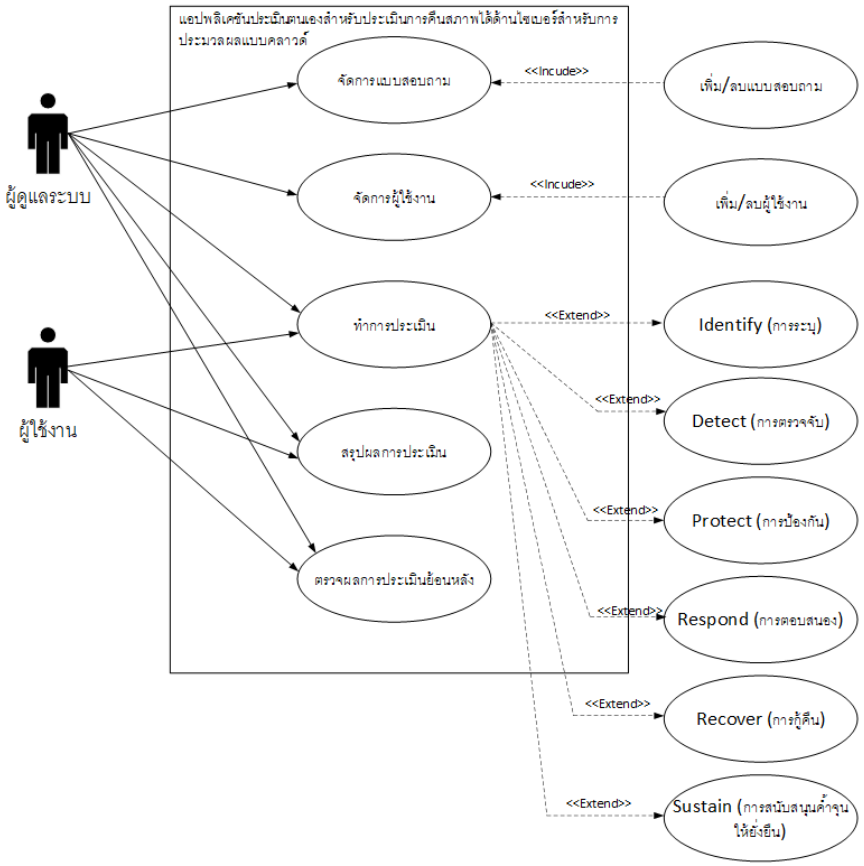
	Strategy					
	Practice					
	Identify	Protect	Detect	Respond	Recover	Sustain
People	Business Environment	Training	Security Audit	Respond Awareness	Recovery Awareness	Cybersecurity Experience
	Risk Management	Security Awareness		Communications		
Process	Confidentiality	Physical Security	Integrity	Respond Plan	Recovery Plan	Availability
	Governance		Analyze			Improvement
	Outsource Management					Change Management
Technology	Vulnerability Management	Critical Infrastructure Protect	Monitoring	Incident Response	Recovery Point Objective	Centralized Management
	Penetration Testing	Access Control			Recovery Time Objective	Continuous Operation
					Hight Avalible	

3.1.3 ขั้นตอนที่ 3 : เพื่อให้บรรลุตามวัตถุประสงค์ข้อที่ 3

จากผลการศึกษาจากวัตถุประสงค์ข้อที่ 1 และผลจากการพัฒนากรอบการคืนสภาพได้สำหรับการประมวลผลแบบคลาวด์ และการออกแบบการประเมินตนเองตามวัตถุประสงค์ข้อที่ 2 จะถูกนำมาสรุปผ่านแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ ที่สามารถแสดงผลในลักษณะ กราฟเรดาร์ (Radar Chart) โดยแยกหัวข้อในการประเมินตนเองเป็น การระบุ (Identify) การตรวจจับ (Detect), การป้องกัน (Protect), การตอบสนอง (Respond), การคืนสภาพ (Recover) และการสนับสนุนค้ำจุนให้ยั่งยืน (Sustain)

3.1.4 วิเคราะห์และออกแบบระบบในเชิงวัตถุ

โดยใช้หลักของ Use Case Diagram ในการออกแบบการสร้างระบบเพื่อแสดงความสัมพันธ์ของผู้ที่เกี่ยวข้องในระบบ ดังภาพประกอบที่ 3.1



ภาพประกอบที่ 3.1 Use Case Diagram แสดงความสัมพันธ์ของผู้ใช้งานระบบ

3.2 เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยได้กำหนดให้มีเครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย ดังนี้

3.3.1 เครื่องมือในการวิจัย

1) แบบประเมินตนเองเกี่ยวกับการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์

3.3.2 ฮาร์ดแวร์ที่ใช้ในการวิจัยประกอบด้วย

1) คอมพิวเตอร์แบบตั้งโต๊ะหรือแบบพกพาที่มีซีพียูไม่ต่ำกว่า Intel Core 2 Duo
2) ฮาร์ดดิสก์ที่มีความจุไม่ต่ำกว่า 120 GB
3) หน่วยความจำไม่ต่ำกว่า 2 GB

3.3.3 ซอฟต์แวร์ที่ใช้ในการวิจัยประกอบด้วย

1) ระบบปฏิบัติการ Microsoft Windows / iOS / Android (PC, Notebook, Smart Devices) สำหรับเป็นเครื่องมือที่ใช้ในการพัฒนาโปรแกรมระบบ
2) ระบบจัดการฐานข้อมูล MySQL Database สำหรับติดตั้งฐานข้อมูล
3) Apache HTTP Server สำหรับติดตั้งเครื่องบริการเว็บ
4) โปรแกรมในการพัฒนาระบบ ใช้ภาษา VB
5) NETSPSS for Windows

3.3.4 เครื่องบริการ (Server) ที่มีคุณลักษณะดังต่อไปนี้

1) รองรับระบบปฏิบัติการ Windows หรือ Linux
2) รองรับการใช้งาน ภาษา ASP ASP.NET PHP หรือ JSP
3) รองรับการใช้งานฐานข้อมูล MySQL หรือ MS Access
4) มีพื้นที่ใช้งานไม่น้อยกว่า 100 MB

3.3 การกำหนดเกณฑ์พิจารณาระดับค่าคะแนน

3.3.1 การกำหนดระดับค่าคะแนนของแบบประเมินตนเอง

ระดับคะแนนของมาตรวัดตามมาตราส่วนประมาณค่ากำหนดระดับค่าคะแนนในการตอบแบบประเมินตนเองเกี่ยวกับการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ 5 ระดับดังนี้

ระดับมากที่สุด	ให้น้ำหนักคะแนนเป็น	5 คะแนน
ระดับมาก	ให้น้ำหนักคะแนนเป็น	4 คะแนน
ระดับปานกลาง	ให้น้ำหนักคะแนนเป็น	3 คะแนน
ระดับน้อย	ให้น้ำหนักคะแนนเป็น	2 คะแนน
ระดับน้อยที่สุด	ให้น้ำหนักคะแนนเป็น	1 คะแนน

3.3.2 การแปลความหมายระดับค่าคะแนนเฉลี่ยของแบบประเมินตนเอง

การแปลความหมายระดับค่าคะแนนเฉลี่ยของข้อมูลที่เก็บได้จากแบบประเมินตนเอง ข้อมูลวัดมาตราส่วนประมาณค่าพิจารณาตามช่วงคะแนนสำหรับการแปลผลดังนี้

ระดับคะแนนเฉลี่ย	4.50 - 5.00	หมายถึง	มีระดับมากที่สุด
ระดับคะแนนเฉลี่ย	3.50 - 4.49	หมายถึง	มีระดับมาก

ระดับคะแนนเฉลี่ย 2.50 - 3.49 หมายถึง มีระดับปานกลาง
ระดับคะแนนเฉลี่ย 1.50 - 2.49 หมายถึง มีระดับน้อย
ระดับคะแนนเฉลี่ย 1.00 - 1.49 หมายถึง มีระดับน้อยที่สุด

3.3.3 การแปลความหมายระดับค่าคะแนนเฉลี่ยของดัชนีความสอดคล้องของข้อคำถาม

ระดับค่าคะแนนดัชนีความสอดคล้องของข้อคำถามที่ใช้ในการสอบถามความคิดเห็นจากผู้เชี่ยวชาญ โดยใช้การแปลความหมายระดับค่าคะแนนเฉลี่ยเป็น 2 ระดับ ดังนี้

ระดับคะแนนเฉลี่ย -1.00 - 0.49 หมายถึงมีระดับความสอดคล้องไม่เหมาะสม
ระดับคะแนนเฉลี่ย -1.00 - 0.49 หมายถึงมีระดับความสอดคล้องไม่เหมาะสม

3.4 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลการวิจัย ข้อมูลดำเนินการโดยนำผลการประเมินตนเองมาวิเคราะห์แล้วประเมินผลข้อมูลโดยใช้โปรแกรมสำเร็จรูป SPSS (Statistics Package for the Social Sciences : SPSS) เพื่อใช้ในการวิเคราะห์และรายงานผลค่าทางสถิติ และประมวลผลหาความสัมพันธ์ทางสถิติด้วยระดับความเชื่อมั่น 95 เปอร์เซ็นต์ และมีความคลาดเคลื่อนที่ยอมรับได้ 0.05 เปอร์เซ็นต์ เป็นเกณฑ์ในการยอมรับหรือปฏิเสธสมมติฐานในการศึกษา
สถิติที่ใช้ในการวิเคราะห์

1. ค่าเฉลี่ย หาค่าเฉลี่ยของคะแนนการประเมินโดยคำนวณจากสูตร ดังนี้

$$\bar{x} = \frac{\sum x}{n}$$

เมื่อ $\bar{x}$ แทน ค่าเฉลี่ย
$\sum x$ แทน ผลรวมของคะแนนทั้งหมด
N แทน จำนวนข้อมูลทั้งหมด

2. ความเบี่ยงเบนมาตรฐาน (Standard Deviation) คำนวณจากสูตรดังนี้

เมื่อ $S.D. = \sqrt{\frac{\sum (x-\bar{x})}{n}}$

	S.D.	แทน	ส่วนเบี่ยงเบนมาตรฐาน
	X	แทน	ค่าของข้อมูลแต่ละตัว
	$\bar{x}$	แทน	ค่าเฉลี่ยของกลุ่มตัวอย่าง
	N	แทน	จำนวนตัวอย่าง

3.5 การวิเคราะห์ออกแบบบระบบ

ผู้วิจัยได้เลือกการออกแบบระบบในแบบ Software Development Life Cycle (SDLC) ตั้งแต่ต้นจนจบการพัฒนาระบบ ซึ่ง SDLC นั้นสามารถแสดงได้ ดังภาพประกอบที่ 3-3

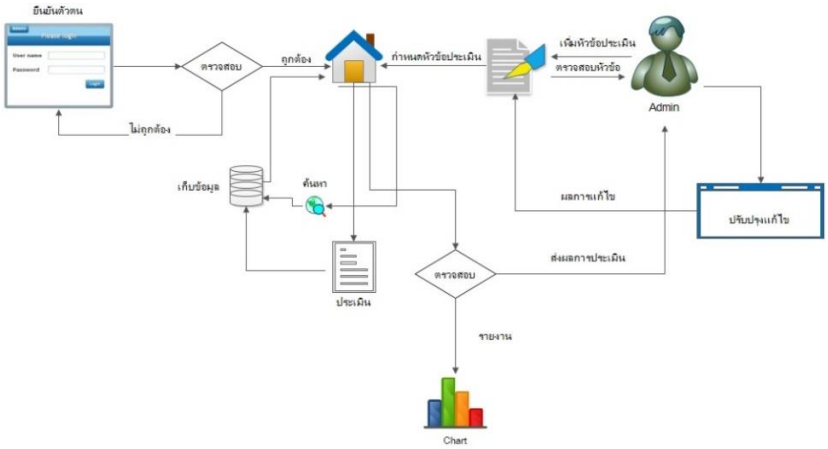
ภาพประกอบที่ 3.2 Software Development Life Cycle (SDLC)

ซึ่งการออกแบบระบบในรูปแบบ SDLC นั้นมีทั้งสิ้น 7 ขั้นตอนดังนี้

1) เข้าใจปัญหา (Problem Recognition) ในส่วนนี้ผู้วิจัยได้ศึกษาปัญหาต่าง ๆ ที่เกิดขึ้นจากการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งความสามารถในคืนสภาพ ที่รองรับการให้การบริการแบบคลาวด์ในปัจจุบัน

2) ศึกษาความเป็นไปได้ (Feasibility Study) ในขั้นตอนนี้ผู้วิจัยได้รวบรวมข้อมูลดิบต่าง ๆ จาก งานวิจัย และสัมภาษณ์ผู้เชี่ยวชาญเพื่อหาแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ต่อไปได้
3) วิเคราะห์ (Analysis) ผู้วิจัยวิเคราะห์ข้อมูลต่าง ๆ ที่ได้จากการรวบรวม รวมทั้งหาความสัมพันธ์ระหว่างข้อคำถาม
4) ออกแบบ (Design) ผู้วิจัยได้สร้างข้อคำถามต่าง ๆ ออกแบบหน้าจอโปรแกรม รวมทั้งหน้าจอแสดงรายงานต่าง ๆ
5) สร้างหรือพัฒนาระบบ (Development) ผู้วิจัยได้พัฒนาแอปพลิเคชันประเมินตนเองในลักษณะ Web Application บนเว็บเซิร์ฟเวอร์ เพื่อให้ผู้ใช้สามารถเข้าถึงได้จากทุกที่ รวมทั้งมีประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ ที่สามารถแสดงผลในลักษณะ กราฟเรดาร์ (Radar Chart) โดยแยกหัวข้อในการประเมินเป็น การระบุ (Identify), การป้องกัน (Protect), การตรวจจับ (Detect), การตอบสนอง (Respond), การคืนสภาพ (Recover)
6) การนำไปใช้ (Implementation) ผู้วิจัยได้นำระบบให้ผู้บริหารระดับสูง ผู้กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และ ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
7) บำรุงรักษา (Maintenance) ผู้วิจัยได้จัดทำการประเมินความพึงพอใจของระบบ และการสอบถามจากผู้ใช้เพื่อหาจุดบกพร่องในระบบเพื่อแก้ไขให้เหมาะสมกับผู้ใช้มากที่สุด นอกจากนี้ ผู้วิจัยได้ดำเนินการสำรองข้อมูลทุกสัปดาห์ รวมทั้งรวบรวมข้อมูลคำแนะนำที่ได้จากผู้ใช้ระหว่างการเปิดใช้งานระบบจริงมาปรับปรุงและบำรุงรักษาต่อไป

วงจรโดยรวมของการแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีภาพรวมของระบบการพัฒนา ดังภาพประกอบที่ 3.3



ภาพประกอบที่ 3.3 วงจรโดยรวมของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

3.6 ระยะเวลาในการดำเนินการ

การดำเนินงานวิจัยใช้ระยะเวลารวมทั้งสิ้น 12 เดือน ตั้งแต่เดือน กันยายน พ.ศ.2560 ถึงเดือนสิงหาคม พ.ศ.2561 ดังตารางประกอบที่ 3.2

ตารางประกอบที่ 3.2 ระยะเวลาในการดำเนินงาน

ลำดับ	ขั้นตอนการดำเนินงาน	1	2	3	4	5	6	7	8	9	10	11	12
		ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.
		2560				2561							
1	ศึกษาปัญหา												
2	รวบรวมข้อมูลจากเอกสารและงานวิจัยที่เกี่ยวข้อง												
3	ทำการวิจัยและพัฒนาระบบประเมิน												
4	ผลการวิจัยและข้อเสนอแนะ												
5	เรียบเรียงและปรับปรุงงานวิจัย												
6	นำเสนอผลงานและจัดทำเอกสารวิจัย												

3.7 สรุป

ในบทที่ 3 นี้เป็นการนำเสนอวิธีดำเนินการวิจัย ที่ประกอบด้วย การออกแบบการวิจัย ขั้นตอนการวิจัย เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย กลุ่มตัวอย่าง การเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล การกำหนดเกณฑ์พิจารณาระดับค่าคะแนน และระยะเวลาในการดำเนินงาน เพื่อตอบคำถามตามวัตถุประสงค์และสมมติฐานที่กำหนดไว้

บทที่ 4
ผลการวิจัย

การศึกษาและการวิจัยนี้เป็นแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ (Could Computing) โดยผู้วิจัยได้ทำการศึกษาค้นคว้าเกี่ยวข้องกับความปลอดภัยไซเบอร์ และการคืนสภาพได้ของระบบการประมวลผลแบบคลาวด์ (Could Computing) พร้อมให้ผู้เชี่ยวชาญทำการชี้แนะและให้คำแนะนำที่เกี่ยวข้องเพื่อนำไปพัฒนากรอบการคืนสภาพได้ของระบบการประมวลผลแบบคลาวด์ (Could Computing) และได้ดำเนินการวิเคราะห์และออกแบบระบบเชิงวัตถุด้วยการใช้หลักการของยูสเคส แล้วทำการพัฒนาโปรแกรมสำหรับประเมินการคืนสภาพได้ของระบบการประมวลผลแบบคลาวด์ หลังจากนั้นได้ใช้ระบบทำการประเมินฝั่งของผู้ให้บริการคลาวด์

การวิจัยครั้งนี้มีวัตถุประสงค์ 3 ข้อ ดังนี้

1. เพื่อวิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

2. เพื่อพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

3. เพื่อพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1

จากวัตถุประสงค์งานวิจัยข้อที่ 1 ผู้วิจัยได้ดำเนินการตามวัตถุประสงค์โดยมีขั้นตอนการดำเนินการดังนี้

ขั้นตอนที่ 1 ศึกษา ค้นคว้าเกี่ยวกับเรื่องความปลอดภัยไซเบอร์ และการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ผลของการศึกษา ค้นคว้าพบว่าแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ จะต้องพิจารณาด้านต่าง ๆ ดังนี้ 1. การระบุ (Identify), 2. การป้องกัน (Protect), 3. การตรวจจับ (Detect), 4. การตอบสนอง (Respond), 5. การคืนสภาพ (Recover), 6. การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) โดยแต่ละด้านมีความสัมพันธ์เชื่อมโยงกับคน กระบวนการ และเทคโนโลยี ไม่ทางใดก็ทางหนึ่ง และปัจจัยที่ใช้ประกอบการพิจารณาซึ่งแยกย่อย

อยู่ในหัวข้อต่าง ๆ นั้น จะถูกจัดทำขึ้นตามความเหมาะสมขององค์กรให้อยู่ในเกณฑ์ที่รับได้ แต่จะเน้นไปที่เรื่องของ CIA คือ Confidentiality (ความลับ), Integrity (ความถูกต้อง) และ Availability (ความพร้อมใช้) ซึ่งแยกเป็นแนวทางในด้านนโยบายและปฏิบัติ

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 2

จากวัตถุประสงค์งานวิจัยข้อที่ 2 พัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ผู้วิจัยได้สัมภาษณ์เชิงลึกและสนทนากลุ่มกับผู้เชี่ยวชาญถึงเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ กับผู้เชี่ยวชาญจำนวน 6 ท่านได้แก่

ผู้เชี่ยวชาญ ท่านที่ 1

ชื่อ นาย เอกฉัตร **นามสกุล** บ่ายคล้อย

ตำแหน่ง กรรมการผู้จัดการ **บริษัท/หน่วยงาน** EP&IT Solution Co., Ltd.

ผู้เชี่ยวชาญ ท่านที่ 2

ชื่อ อาจารย์ นนทวัตต์ **นามสกุล** สาระมาน

ตำแหน่ง President **บริษัท/หน่วยงาน** สมาคม CIPAT ไซปัด

ผู้เชี่ยวชาญ ท่านที่ 3

ชื่อ นาย นริส **นามสกุล** อุไรพันธ์

ตำแหน่ง Project Manager **บริษัท/หน่วยงาน** Triangle Soft Co., Ltd.

ผู้เชี่ยวชาญ ท่านที่ 4

ชื่อ อาจารย์ ศรายุท **นามสกุล** ฉายสุริยะ

ตำแหน่ง กรรมการผู้จัดการ **บริษัท/หน่วยงาน** NYSIIS Solutions Co., Ltd.

ผู้เชี่ยวชาญ ท่านที่ 5

ชื่อ นาย เกรียงไกร **นามสกุล** ศรีสุวรรณ

ตำแหน่ง Senior Security Specialist **บริษัท/หน่วยงาน** EP&IT Solution Co., Ltd.

ผู้เชี่ยวชาญ ท่านที่ 6

ชื่อ นาย ชัยพร **นามสกุล** ทบแป

ตำแหน่ง ผู้ช่วยผู้จัดการฝ่ายพัฒนาผลิตภัณฑ์ธุรกิจอิเล็กทรอนิกส์

บริษัท/หน่วยงาน กสท. โทรคมนาคม จำกัด (มหาชน)

จากการสัมภาษณ์พบว่าความปลอดภัยไซเบอร์แบบดั้งเดิมมุ่งเน้นไปที่การป้องกัน ซึ่งปัจจุบันแนวโน้มการโจมตีทางไซเบอร์มีความรุนแรง และ ใช้วิธีการโจมตีที่ฉลาดมากขึ้นทำให้การป้องกันในปัจจุบันไม่เพียงพอ การเปลี่ยนแปลงนี้ยังต้องการการบริหารความเสี่ยงที่มีประสิทธิภาพมาก ปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์เป็นปัญหาสำคัญที่จะต้องมีบริหารจัดการแบบเป็นขั้นตอน และการที่จะพัฒนาการคืนสภาพของระบบการประมวลผลแบบคลาวด์ ต้องเริ่มจากการกำหนดนโยบายและกลยุทธ์เพื่อบริหารจัดการ คน กระบวนการ และเทคโนโลยี เมื่อกำหนดนโยบายและกลยุทธ์ไว้ขั้นตอนต่อไปคือการออกแบบทุกสิ่งทุกอย่างที่จำเป็น เปลี่ยนกลยุทธ์ให้เป็นความจริง ออกแบบที่ดีจะเป็นรากฐานที่มั่นคงเพื่อให้แน่ใจได้ว่ากระบวนการสามารถใช้งานได้ในภายหลังและเป็นไปตามความจำเป็นขององค์กร สามารถเปลี่ยนสภาพแวดล้อมการดำเนินงานได้อย่างมีประสิทธิภาพ และสร้างการตระหนักถึงหน้าที่และความรับผิดชอบของทุกคนมีส่วนขับเคลื่อนในการพัฒนาระดับของการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการปรับปรุงอย่างต่อเนื่องไม่ใช่แค่เรื่องที่กำลังดำเนินการอยู่เท่านั้น ทุกอย่างที่องค์กรทำควรอยู่ภายใต้กระบวนการของความเข้าใจและการปรับปรุง ในทำนองเดียวกันองค์กรควรปรับปรุงกลยุทธ์อย่างต่อเนื่องให้ทันต่อยุคสมัย เทคโนโลยี และภัยคุกคาม หลังจากที่สามารถพัฒนาระดับความปลอดภัยไซเบอร์ให้อยู่ในเกณฑ์ที่รับได้แล้ว การรักษาสภาพให้ดำรงอยู่เป็นปัจจัยสำคัญสำหรับการดำเนินงานในระยะยาว โดยสามารถแสดงผลแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ดังตารางที่ 4.1

ตารางที่ 4.1 กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

	Strategy					
	Practice					
	Identify	Protect	Detect	Respond	Recover	Sustain
People	Business Environment	Training	Security Audit	Respond Awareness	Recovery Awareness	Cybersecurity Experience
	Risk Management	Security Awareness		Communications		
Process	Confidentiality	Physical Security	Integrity	Respond Plan	Recovery Plan	Availability
	Governance		Analyze			Improvement
	Outsource Management					Change Management
Technology	Vulnerability Management	Critical Infrastructure Protect	Monitoring	Incident Response	Recovery Point Objective	Centralized Management
	Penetration Testing	Access Control			Recovery Time Objective	Continuous Operation
					Hight Avalible	

จากการสัมภาษณ์ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ และแนวคิดทฤษฎีที่เกี่ยวข้องผู้วิจัยได้นำมาจัดทำแบบประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ของหน่วยงานที่ให้บริการระบบประมวลผลแบบคลาวด์ภายในประเทศจำนวน 3 หน่วยงาน โดยมีกลุ่มตัวอย่างจำนวนรวมทั้งหมด 120 คน ซึ่งเป็นบุคลากรที่เกี่ยวข้องกับการปฏิบัติงานทางด้านความมั่นคงปลอดภัยไซเบอร์ของระบบการให้บริการประมวลผลแบบคลาวด์ โดยแยกหัวข้อการประเมินเป็น 6 หัวข้อคือ 1. การระบุ (Identify), 2. การป้องกัน (Protect), 3. การตรวจจับ (Detect), 4. การตอบสนอง (Respond), 5. การคืนสภาพ (Recover) 6. การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) พบว่า หน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์หน่วยงานที่ 1 มีค่าเฉลี่ยรวมเท่ากับ 3.55 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.85 ระดับการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์อยู่ในระดับ มาก โดยสามารถแสดงผลของการประเมิน ดังตารางที่ 4.2

ตารางประกอบที่ 4.2 แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์ สำหรับระบบการประมวลผลแบบคลาวด์ของ หน่วยงานที่ 1

หน่วยงานให้บริการระบบการประมวลผลแบบคลาวด์ หน่วยงานที่ 1				
ลำดับ	รายการประเมิน	$\bar{X}$	S.D.	การแปลผล
1	การระบุ (Identify)	3.40	0.84	ปานกลาง
2	การตรวจจับ (Detect)	3.02	0.84	ปานกลาง
3	การป้องกัน (Protect)	3.58	0.82	มาก
4	การตอบสนอง (Respond)	3.97	0.82	มาก
5	การกู้คืน (Recover)	4.09	0.88	มาก
6	การสนับสนุน (Sustain)	3.21	0.89	ปานกลาง
	ผลรวม	3.55	0.85	มาก

หน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์หน่วยงานที่ 2 มีค่าเฉลี่ยรวมเท่ากับ 3.51 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.76 ระดับการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์อยู่ในระดับ มาก โดยสามารถแสดงผลของการประเมิน ดังดังตารางประกอบที่ 4.3

ตารางประกอบที่ 4.3 แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์ สำหรับระบบการประมวลผลแบบคลาวด์ของ หน่วยงานที่ 2

หน่วยงานให้บริการระบบการประมวลผลแบบคลาวด์ หน่วยงานที่ 2				
ลำดับ	รายการประเมิน	$\bar{X}$	S.D.	การแปลผล
1	การระบุ (Identify)	3.48	0.71	มาก
2	การตรวจจับ (Detect)	3.50	0.78	มาก
3	การป้องกัน (Protect)	3.41	0.78	มาก
4	การตอบสนอง (Respond)	3.45	0.80	มาก
5	การกู้คืน (Recover)	4.02	0.71	มาก
6	การสนับสนุน (Sustain)	3.18	0.79	ปานกลาง
	ผลรวม	3.51	0.76	มาก

หน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์หน่วยงานที่ 3 มีค่าเฉลี่ยรวมเท่ากับ 3.54 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.79 ระดับการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์อยู่ในระดับ มาก โดยสามารถแสดงผลของการประเมิน ดังตารางประกอบที่ 4.4

ตารางประกอบที่ 4.4 แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์ สำหรับระบบการประมวลผลแบบคลาวด์ของ หน่วยงานที่ 3

หน่วยงานให้บริการระบบการประมวลผลแบบคลาวด์ หน่วยงานที่ 3				
ลำดับ	รายการประเมิน	$\bar{X}$	S.D.	การแปลผล
1	การระบุ (Identify)	3.34	0.71	ปานกลาง
2	การตรวจจับ (Detect)	3.43	0.76	มาก
3	การป้องกัน (Protect)	3.81	0.83	มาก
4	การตอบสนอง (Respond)	3.23	0.77	ปานกลาง
5	การกู้คืน (Recover)	4.08	0.88	มาก
6	การสนับสนุน (Sustain)	3.36	0.79	ปานกลาง
	ผลรวม	3.54	0.79	มาก

สรุปผลรวมการประเมินตนเองของหน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์จำนวน 3 หน่วยงาน มีค่าเฉลี่ยรวมเท่ากับ 4.15 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.85 ระดับการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์อยู่ในระดับ มาก โดยสามารถแสดงผลของการประเมิน ดังตารางประกอบที่ 4.5

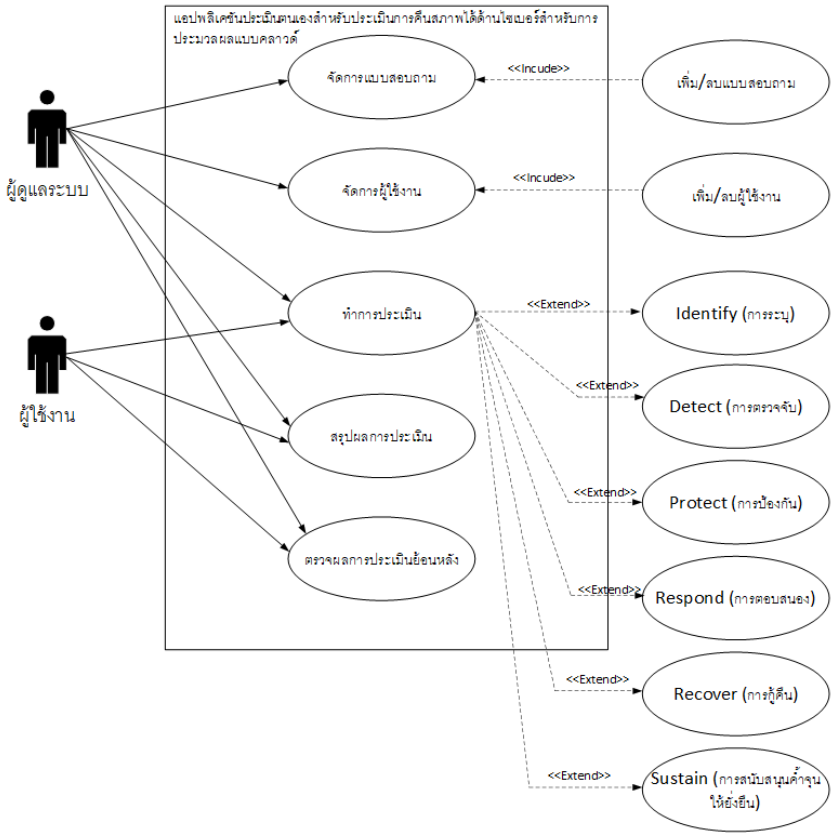
ตารางประกอบที่ 4.5 แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานผลการ ประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์ สำหรับระบบการประมวลผลแบบคลาวด์โดยรวมของ 3 หน่วยงาน

สรุปผลการประเมิน 3 หน่วยงาน				
ลำดับ	**รายการประเมิน**	$\bar{X}$	**S.D.**	**การแปลผล**
1	การระบุ (Identify)	3.41	0.75	ปานกลาง
2	การตรวจจับ (Detect)	3.32	0.76	ปานกลาง
3	การป้องกัน (Protect)	3.60	0.83	มาก
4	การตอบสนอง (Respond)	3.55	0.97	มาก
5	การกู้คืน (Recover)	4.06	0.88	มาก
6	การสนับสนุน (Sustain)	3.25	0.79	ปานกลาง
	ผลรวม	3.53	0.83	มาก

ผลการวิจัยตามวัตถุประสงค์ข้อที่ 3

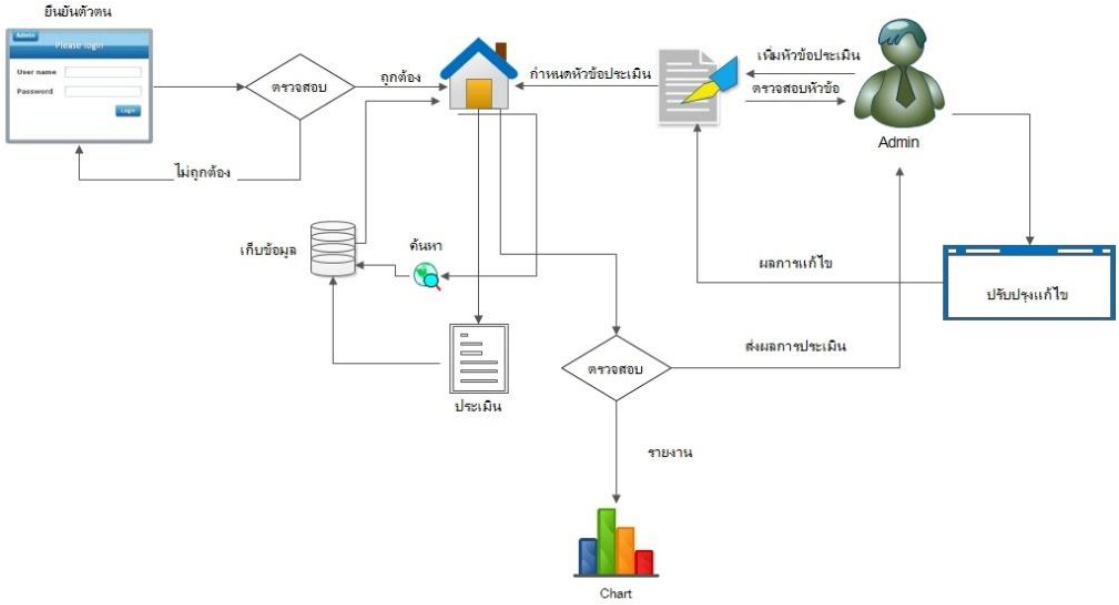
จากวัตถุประสงค์งานวิจัยข้อที่ 3 พัฒนาแอปพลิเคชันสำหรับประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ขั้นตอนที่ 1 ผู้วิจัยได้ออกแบบ โดยใช้หลักของ Use Case Diagram ในการออกแบบการสร้างระบบ เพื่อแสดงความสัมพันธ์ของผู้ที่เกี่ยวข้องในระบบ ดังภาพประกอบที่ 4.1



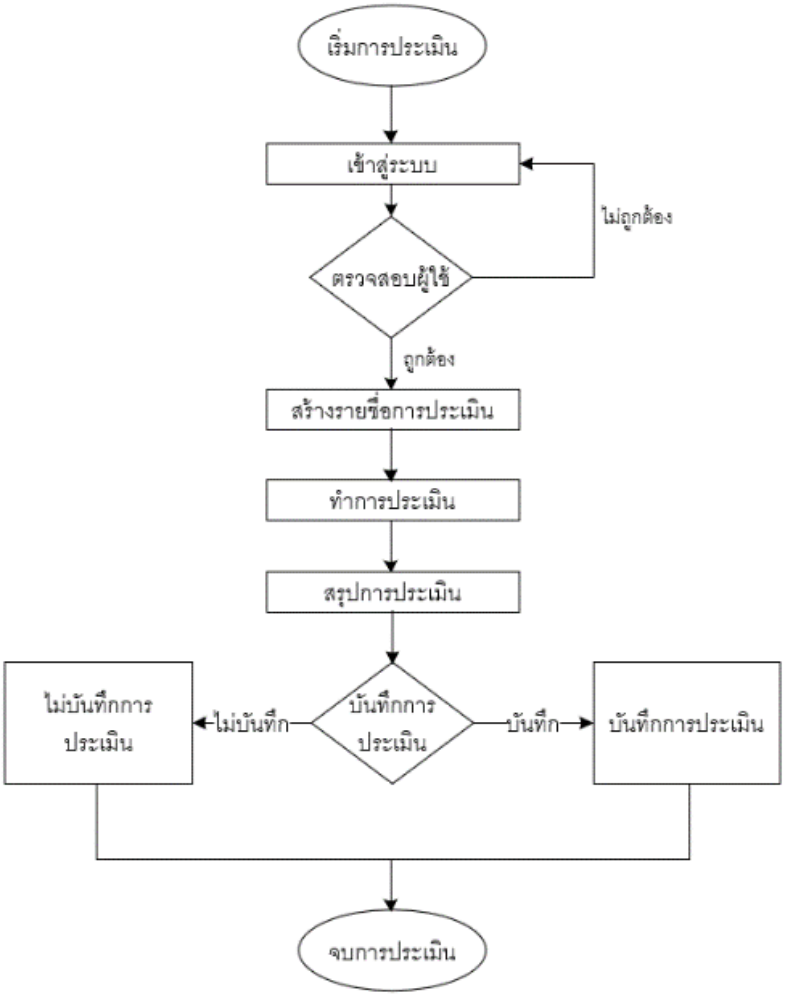
ภาพประกอบที่ 4.1 Use Case Diagram สำหรับแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ขั้นตอนที่ 2 ผู้วิจัยได้ออกแบบวงจรโดยรวมของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์มีภาพรวมของระบบการพัฒนา ดังภาพประกอบที่ 4.2



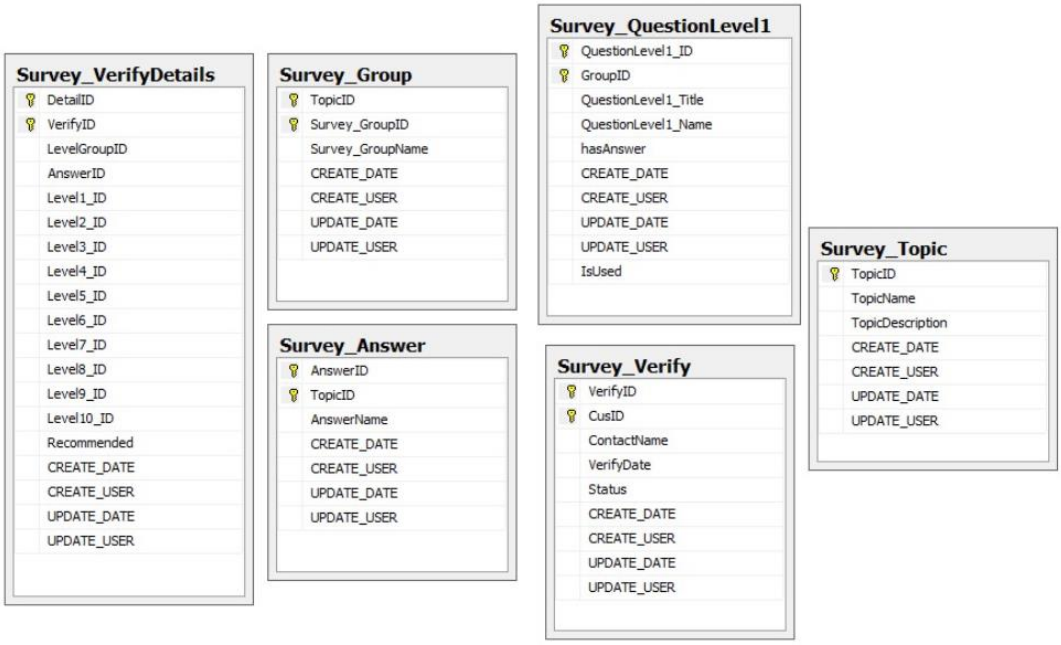
ภาพประกอบที่ 4.2 วงจรโดยรวมของการแนวทางการพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ขั้นตอนที่ 3 ผู้วิจัยได้ออกแบบผังกระบวนการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีกระบวนการประเมิน ดังภาพประกอบที่ 4.3



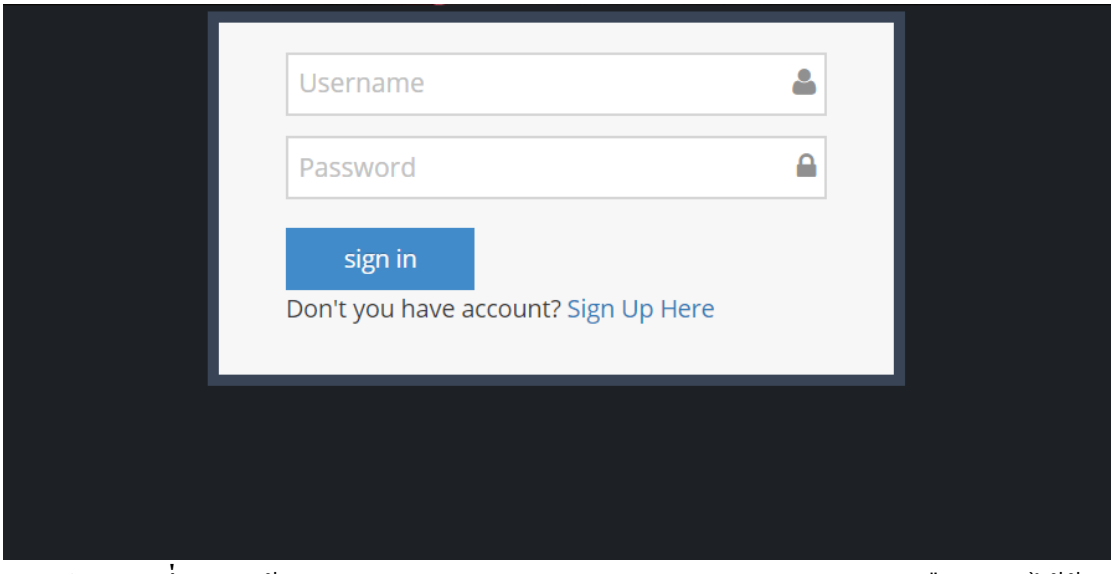
ภาพประกอบที่ 4.3 ผังกระบวนการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ขั้นตอนที่ 4 ผู้วิจัยได้ออกแบบฐานข้อมูลสำหรับแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีกระบวนการประเมิน ดังภาพประกอบที่ 4.4

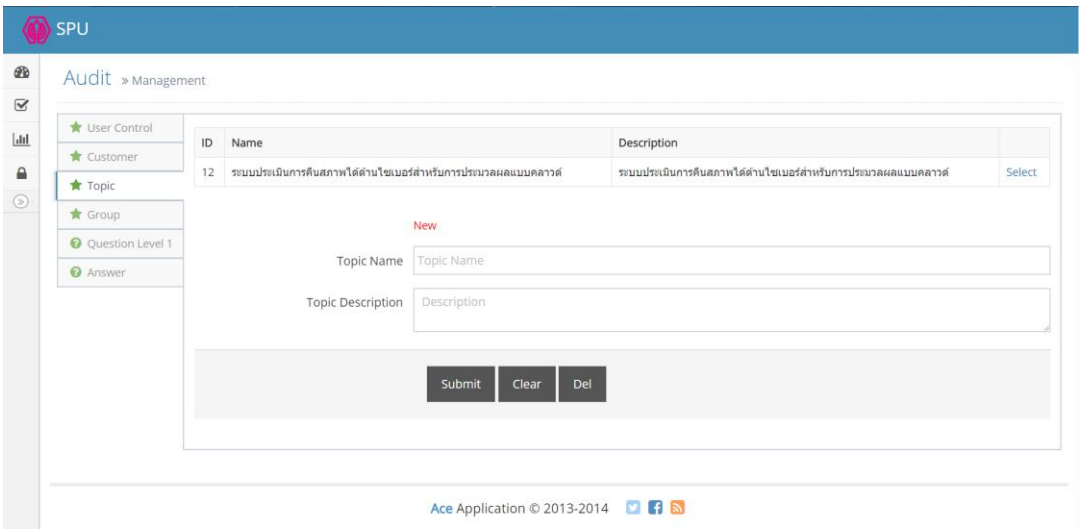


ภาพประกอบที่ 4.4 ฐานข้อมูลสำหรับแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

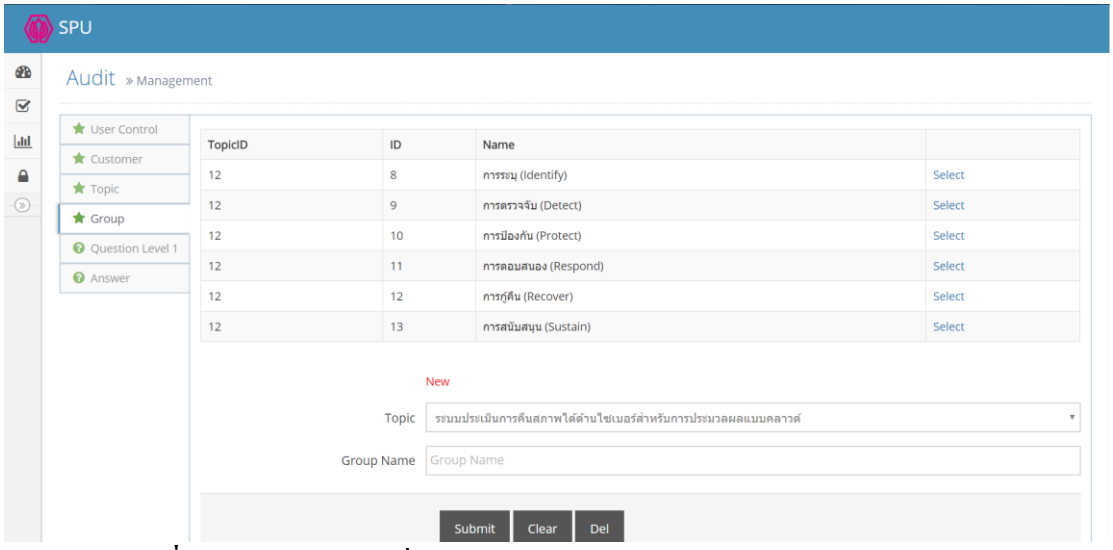
ขั้นตอนที่ 5 ผู้วิจัยได้จัดทำระบบประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ดังภาพประกอบที่ 4.5 – 4.12



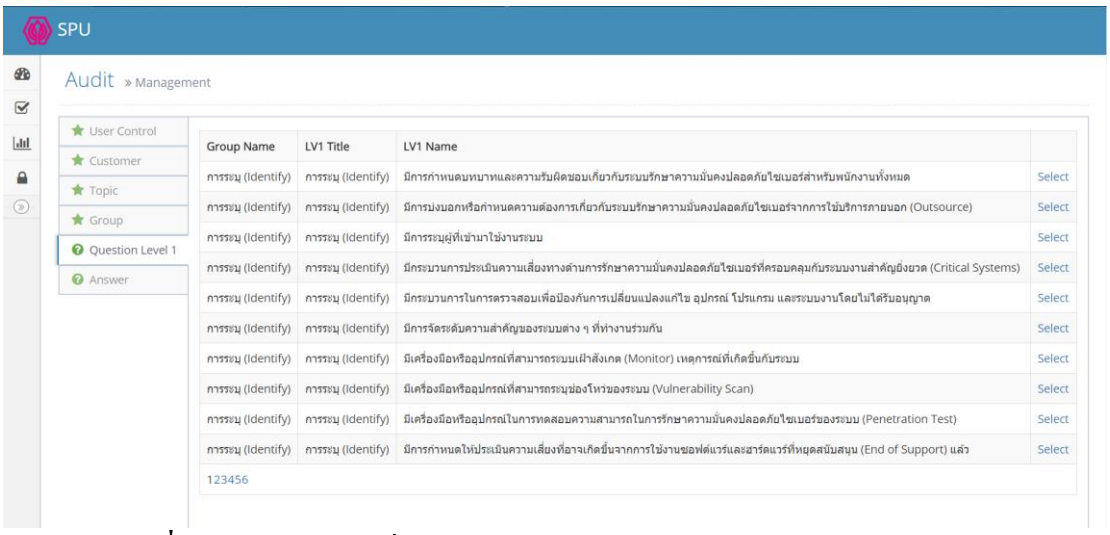
ภาพประกอบที่ 4.5 หน้าแรกของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



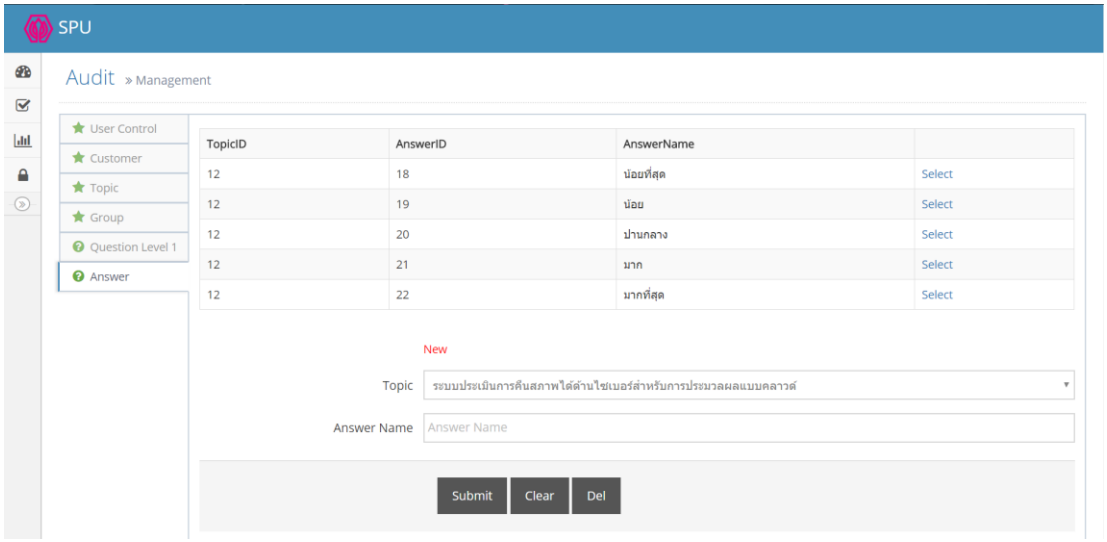
ภาพประกอบที่ 4.6 หน้าสำหรับเพิ่มหัวข้อในการประเมินตนเองสำหรับประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



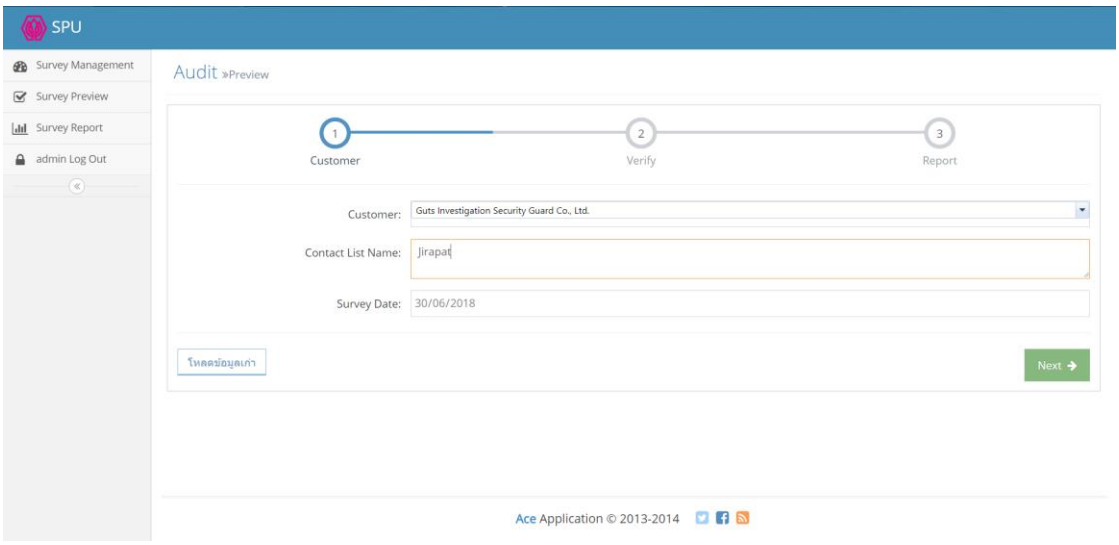
ภาพประกอบที่ 4.7 หน้าสำหรับเพิ่มกลุ่มคำถามในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



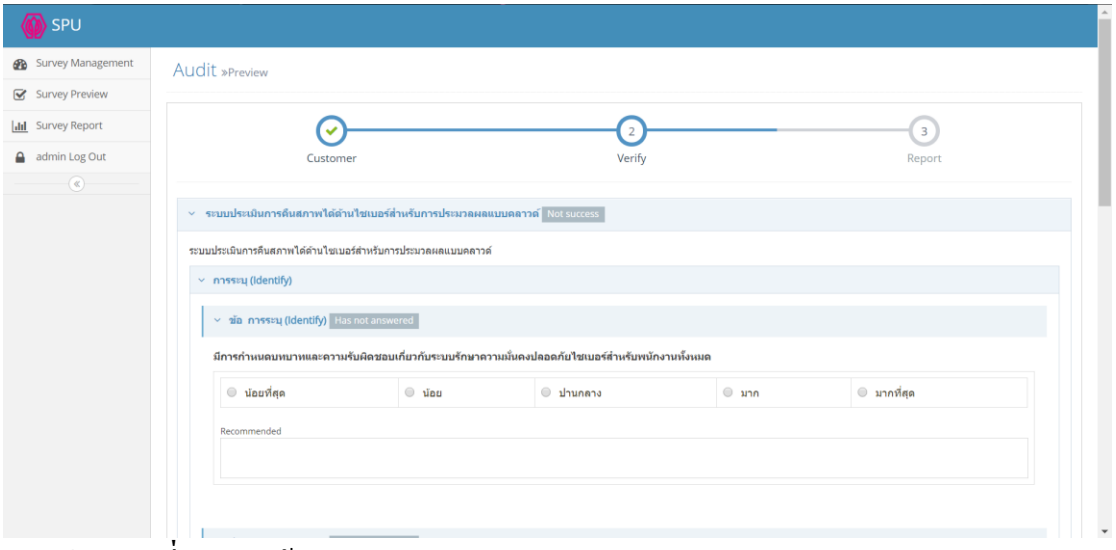
ภาพประกอบที่ 4.8 หน้าสำหรับเพิ่มคำถามในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



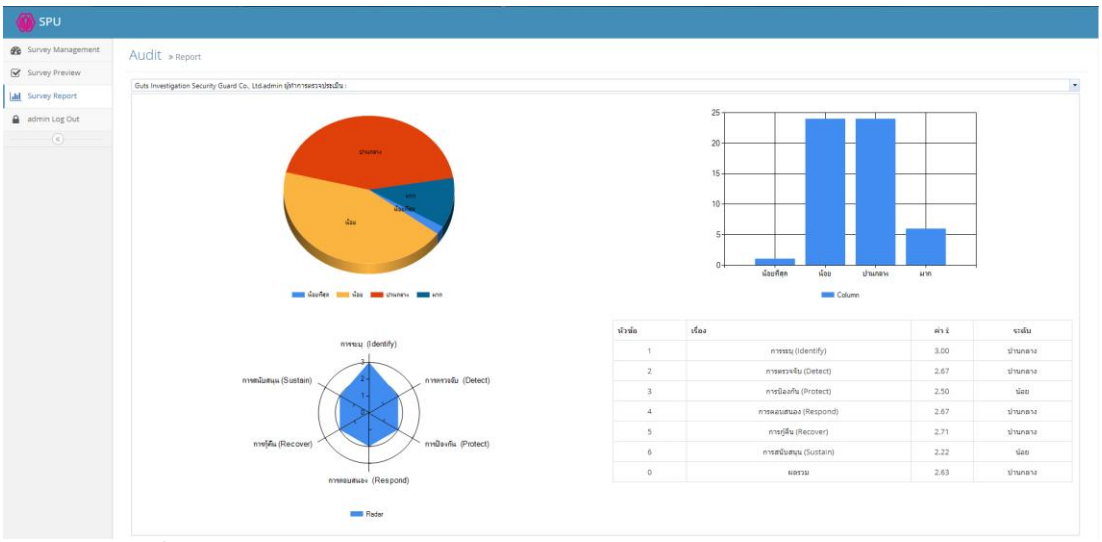
ภาพประกอบที่ 4.9 หน้าสำหรับเพิ่มคำตอบในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



ภาพประกอบที่ 4.10 หน้าสำหรับเพิ่มชื่อบริษัทหรือองค์กรในการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



ภาพประกอบที่ 4.11 หน้าสำหรับทำการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์



ภาพประกอบที่ 4.12 หน้ารายงานผลการประเมินของแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาและวิจัยครั้งนี้ เป็นแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ โดยใช้หลักการกรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework) และโมเดลความมั่นคงปลอดภัยไซเบอร์และความยืดหยุ่นไซเบอร์ (Cybersecurity and Cyber Resilience Model) มาพัฒนาพัฒนาต่อ เพื่อวิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ และพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลแบบคลาวด์ นำเสนอตามลำดับต่อไปนี้

สรุปผลการวิจัย

1. วิเคราะห์ความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

1.1 ผู้วิจัยได้การศึกษาค้นคว้าและสอบถามผู้เชี่ยวชาญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ผลการวิจัยพบว่าความปลอดภัยไซเบอร์แบบดั้งเดิมมุ่งเน้นไปที่การป้องกัน ซึ่งปัจจุบันแนวโน้มการโจมตีทางไซเบอร์มีความรุนแรงและใช้วิธีการโจมตีที่ฉลาดมากขึ้นทำให้การป้องกันในปัจจุบันไม่เพียงพอต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ การเปลี่ยนแปลงนี้จำเป็นที่จะต้องมีการบริหารความเสี่ยงที่มีประสิทธิภาพมาก ปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์เป็นปัญหาสำคัญที่จะต้องมีบริหารจัดการแบบเป็นขั้นตอน และการที่จะพัฒนาไปถึงระดับการคืนสภาพของระบบการประมวลผลแบบคลาวด์นั้น ต้องเริ่มจากการกำหนดนโยบายและกลยุทธ์เพื่อบริหารจัดการ คน กระบวนการ และเทคโนโลยี เมื่อกำหนดนโยบายและกลยุทธ์ไว้ขั้นตอนต่อไปคือการออกแบบทุกสิ่งทุกอย่างที่จำเป็นรวมถึงปัจจัยต่างที่เกี่ยวข้อง เปลี่ยนกลยุทธ์ให้เป็นความจริง การออกแบบที่ดีจะเป็นรากฐานที่มั่นคงของความมั่นคงปลอดภัยไซเบอร์และสามารถยกระดับความมั่นคงปลอดภัยไซเบอร์ให้ไปถึงระดับการคืนสภาพได้ เพื่อให้แน่ใจได้ว่ากระบวนการสามารถใช้งานได้และเป็นไปตามความจำเป็นขององค์กร สามารถเปลี่ยนสภาพแวดล้อมการดำเนินงานได้อย่างมีประสิทธิภาพต้องมีการทดสอบและประเมินผล

ว่าสามารถทำได้สำเร็จตามแนวทางที่วางไว้หรือไม่ และสร้างการตระหนักถึงหน้าที่และความรับผิดชอบของบุคลากรทุกคนที่มีส่วนขับเคลื่อน

ในการพัฒนาระดับของการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะการสนับสนุนจากผู้บริหาร รวมถึงการปรับปรุงอย่างต่อเนื่องไม่ใช่แค่เรื่องที่กำลังดำเนินการอยู่เท่านั้น ทุกอย่างที่องค์กรทำควรอยู่ภายใต้กระบวนการของความเข้าใจและการปรับปรุง ในทำนองเดียวกันองค์กรควรปรับปรุงกลยุทธ์อย่างต่อเนื่องให้ทันต่อยุคสมัย เทคโนโลยี และภัยคุกคาม การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เคยเกิดขึ้น เพื่อเป็นกรณีศึกษาจะสามารถนำผลที่ได้มาประยุกต์ใช้เมื่อต้องรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้ หลังจากที่สามารถพัฒนาระดับความปลอดภัยไซเบอร์ให้อยู่ในเกณฑ์ที่รับได้แล้ว การรักษาสภาพให้ดำรงอยู่เป็นปัจจัยสำคัญสำหรับการดำเนินงานในระยะยาวซึ่งจำเป็นต้องมีการสนับสนุนและการปฏิบัติงานทางด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

2. พัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ผลการวิจัย จากการศึกษาทฤษฎี งานวิจัยที่เกี่ยวข้อง และการสัมภาษณ์ผู้เชี่ยวทางด้านความมั่นคงปลอดภัยไซเบอร์จำนวน 6 ท่าน พบว่าแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ จำเป็นที่จะต้องเริ่มจากการออกนโยบายและแนวทางปฏิบัติเพื่อรองรับระดับการรักษาความปลอดภัยของข้อมูล (Information Security) ความปลอดภัยไซเบอร์ (Cybersecurity) จนไปถึงระดับ การคืนสภาพอย่างรวดเร็ว (Cyber Resilience) หลักของการรักษาความปลอดภัยข้อมูลแบ่งได้เป็นสามส่วนคือ ความลับ (confidentiality) ความสมบูรณ์ (integrity) และความพร้อมใช้ (availability) โดยจะต้องประคับประคองขีดความสามารถที่มีให้ดำเนินอยู่ตลอดเวลา รวมถึงการจัดการความเสี่ยงการประเมินความน่าจะเป็นที่จะเกิดขึ้น และผลกระทบที่อาจเกิดขึ้นการตัดสินใจดำเนินการนี้จะต้องอยู่บนความสมดุลเพื่อป้องกันเหตุการณ์ที่ไม่คาดคิด และจะต้องพิจารณาด้านต่าง ๆ ดังนี้ 1) การระบุ (Identify) 2) การป้องกัน (Protect) 3) การตรวจจับ (Detect) 4) การตอบสนอง (Respond) 5) การคืนสภาพ (Recover) 6) . การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) โดยแต่ละด้านจะต้องสอดคล้องกับการดำเนินงานทางธุรกิจ เพื่อให้ระบบสามารถทำงานได้อย่างถูกต้องโดยสามารถแสดงแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ดังตารางที่ 5.1

ตารางที่ 5.1 กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

	Strategy					
	Practice					
	Identify	Protect	Detect	Respond	Recover	Sustain
People	Business Environment	Training	Security Audit	Respond Awareness	Recovery Awareness	Cybersecurity Experience
	Risk Management	Security Awareness		Communications		
Process	Confidentiality	Physical Security	Integrity	Respond Plan	Recovery Plan	Availability
	Governance		Analyze			Improvement
	Outsource Management					Change Management
Technology	Vulnerability Management	Critical Infrastructure Protect	Monitoring	Incident Response	Recovery Point Objective	Centralized Management
	Penetration Testing	Access Control			Recovery Time Objective	Continuous Operation
					Hight Avalible	

3. พัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวล แบบคลาวด์

3.1 ผู้วิจัยได้จัดทำแบบประเมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์โดยมีผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ให้คำแนะนำและนำไปประเมินผู้ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการระบบคลาวด์ภายในประเทศจำนวน 3 หน่วยงาน โดยมีกลุ่มตัวอย่างจำนวนรวมทั้งหมด 120 คน

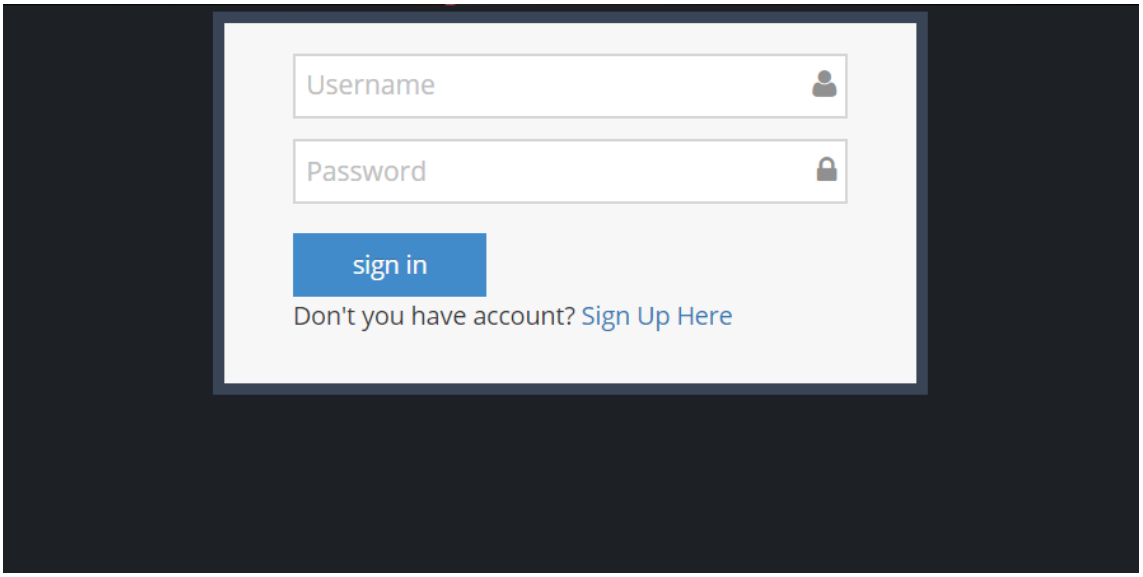
ผลการประเมิน จากการประเมินหน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์จำนวน 3 หน่วยงาน โดยแยกหัวข้อการประเมินเป็น 6 หัวข้อคือ 1) การระบุ (Identify) 2) การป้องกัน (Protect) 3) การตรวจจับ (Detect) 4) การตอบสนอง (Respond) 5) การคืนสภาพ (Recover) 6) . การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) พบว่าผลรวมการประเมินหน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์จำนวน 3 หน่วยงาน มีค่าเฉลี่ยรวมเท่ากับ 3.53 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.83 ระดับการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์อยู่ในระดับ มาก โดยสามารถแสดงผลของการประเมิน ดังตารางที่ 5.2

ตารางที่ 5.2 สรุปค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ผลการประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับระบบการประมวลผลแบบคลาวด์

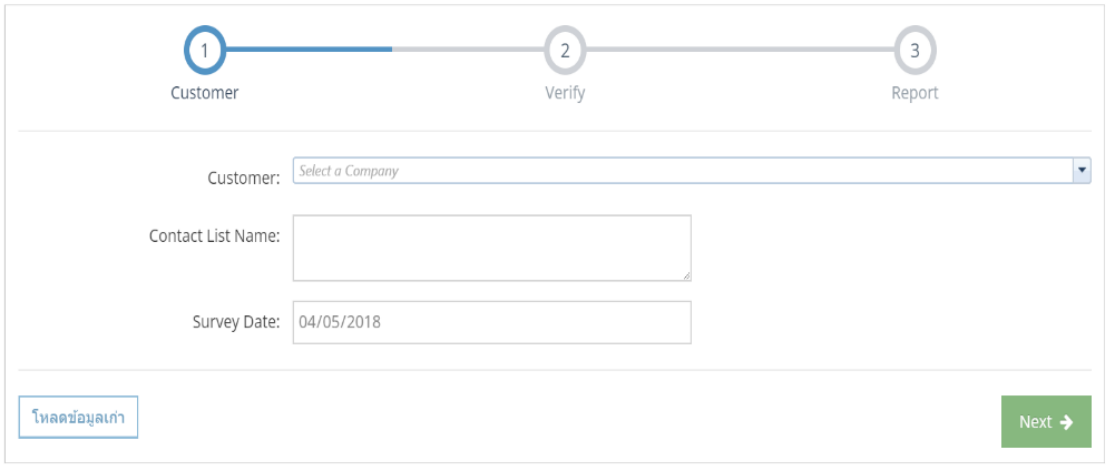
สรุปผลการประเมิน 3 หน่วยงาน				
ลำดับ	รายการประเมิน	$\bar{X}$	S.D.	การแปลผล
1	การระบุ (Identify)	3.41	0.75	ปานกลาง
2	การตรวจจับ (Detect)	3.32	0.76	ปานกลาง
3	การป้องกัน (Protect)	3.60	0.83	มาก
4	การตอบสนอง (Respond)	3.55	0.97	มาก
5	การกู้คืน (Recover)	4.06	0.88	มาก
6	การสนับสนุน (Sustain)	3.25	0.79	ปานกลาง
	ผลรวม	3.53	0.83	มาก

3.1 ผู้วิจัยได้จัดทำแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์โดยใช้ตัวแบบจาก แบบประมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์

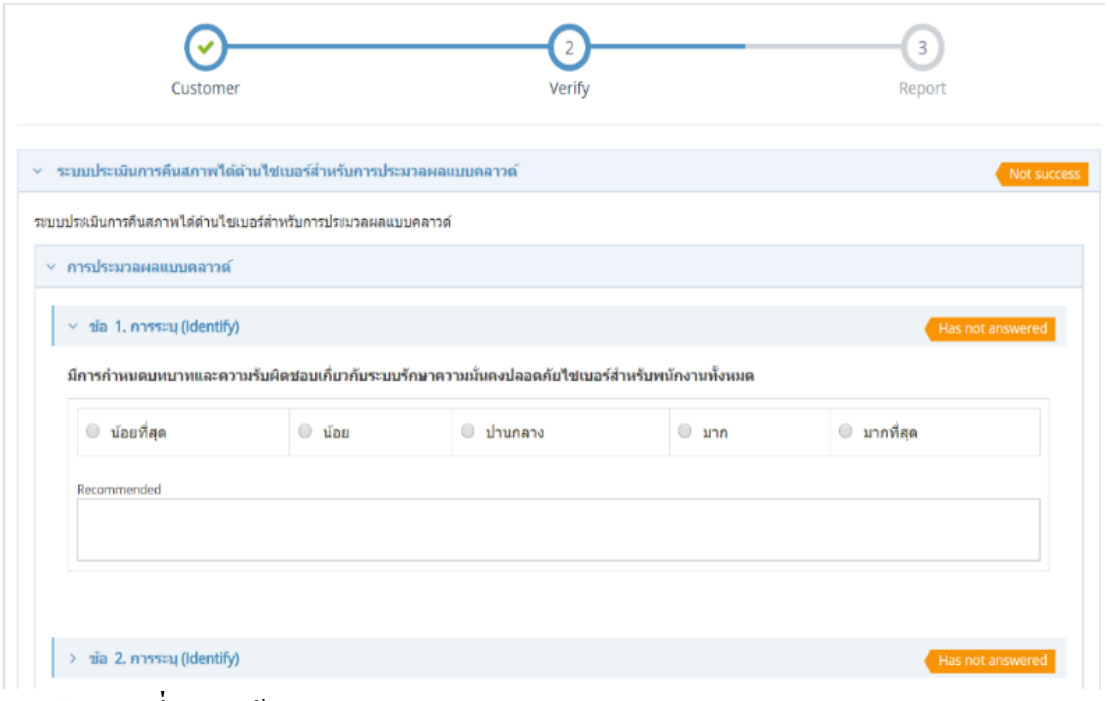
ผลการจัดทำแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ผู้ใช้งานสามารถเข้าสู่ระบบเพื่อทำการประเมินระดับความพร้อมในการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ที่ http://staging.epit.co.th/login เริ่มจากการเข้าสู่ระบบโดยระบบจะตรวจสอบความถูกต้องของ ชื่อผู้ใช่ (Username) และรหัสผ่าน (Password) หลังจากที่เข้าสู่ระบบประเมินเรียบร้อยแล้วจะสามารถ ทำการประเมินได้ หลังจากที่ทำการประเมินเรียบร้อยแล้วสามารถเรียกดูรายงาน (Report) ที่แสดงในรูปแบบกราฟเรดาร์ (Radar Chart) และคะแนนการประเมินในแต่ละหัวข้อได้ โดยสามารถแสดงผลของการจัดทำแอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์ ดังภาพประกอบที่ 5-1 – 5.4



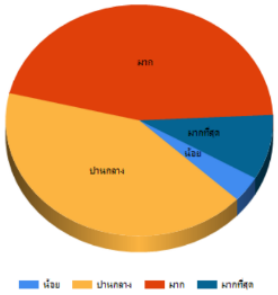
ภาพประกอบที่ 5.1 หน้าเข้าสู่ระบบของแอปพลิเคชันประเมินตนเอง

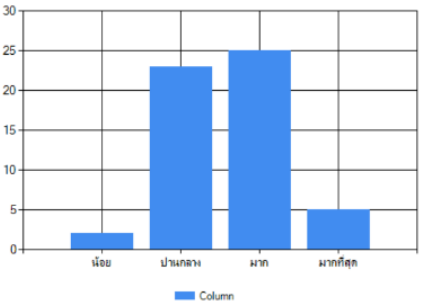


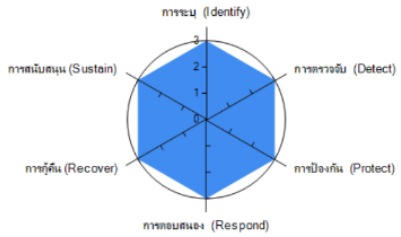
ภาพประกอบที่ 5.2 หน้าเพิ่มชื่อบริษัทหรือองค์กร



ภาพประกอบที่ 5.3 หน้าสำหรับทำการประเมิน







Summary		
ลำดับ	หัวข้อ	ระดับคะแนน
1	การระบุ (Identify)	3.73
2	การตรวจจับ (Detect)	3.78
3	การป้องกัน (Protect)	3.80
4	การตอบสนอง (Respond)	3.44
5	การกู้คืน (Recover)	3.86
6	การสนับสนุน (Sustain)	3.00
0	ผลรวม	3.60

ภาพประกอบที่ 5.4 หน้าสรุปผลการประเมิน

อภิปรายผล

การวิเคราะห์ผลการวิจัยพบว่าการออกแบบในส่วนกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์โดยมีผู้เชี่ยวชาญให้คำแนะนำและเห็นด้วย และมีความสอดคล้องกับแนวคิดของผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์

อย่างไรก็ดี การนำกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ไปใช้งานควรคำนึงถึง 6 ข้อสำคัญได้แก่ 1) การระบุ (Identify) 2) การป้องกัน (Protect) 3) การตรวจจับ (Detect) 4) การตอบสนอง (Respond) 5) การคืนสภาพ (Recover) 6) . การสนับสนุนค้ำจุนให้ยั่งยืน (Sustain) และสภาพแวดล้อมของธุรกิจ เป็นต้น

ปัญหาและอุปสรรค

การวิจัยเรื่อง แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ได้พบปัญหาและอุปสรรคดังนี้

1. ปัญหาจากการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง ซึ่งจำเป็นต้องใช้เวลาที่ศึกษาเพื่อให้เข้าใจในทฤษฎีที่จะต้องนำมาใช้ประกอบการดำเนินการวิจัย เพื่อให้งานวิจัยเกิดคุณภาพและประโยชน์สูงสุดต่อการนำไปใช้ในอนาคต

2. การเข้าดำเนินการสัมภาษณ์ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ ช้าว่ากำหนด เนื่องจากผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์แต่ละท่านมีหน้าที่ความรับผิดชอบในระดับสูงจึงทำให้เวลาไม่ตรงกัน

3. ด้วยหน้าที่การงานของผู้วิจัยที่ลักษณะงานจำเป็นต้องใช้เวลานานในการดำเนินการและต้องมีความต่อเนื่องจึงทำให้เวลาในการทำงานวิจัยมีจำกัด

ข้อเสนอแนะ

1. ข้อเสนอแนะสำหรับการนำงานวิจัยไปใช้จริง

การวิจัยครั้งนี้เป็นแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการระบบการประมวลผลแบบคลาวด์ ไปสู่ระดับการคืนสภาพได้อย่างรวดเร็วของระบบการประมวลผลแบบคลาวด์ งานวิจัยนี้เหมาะสำหรับหน่วยงานที่ให้บริการระบบการประมวลผลแบบคลาวด์

2. ข้อเสนอแนะสำหรับการนำงานวิจัยไปใช้ในอนาคต

กรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์นี้ สามารถนำไปประยุกต์ใช้งานกับบระบบอื่น ๆ ที่นอกเหนือจากระบบการประมวลผลแบบคลาวด์ได้เพราะกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ที่ถูกพัฒนาขึ้นนี้มุ้งเน้นไปที่การพัฒนาการคืนสภาพของโครงสร้างพื้นฐาน (Infrastructure) ซึ่งเป็นพื้นฐานของทุกระบบที่เกิดขึ้นในปัจจุบัน รวมถึงแอปพลิเคชันประเมินตนเองที่จัดทำขึ้นนี้สามารถเพิ่มหัวข้อและข้อคำถามรวมถึงคำตอบที่ใช้ในการประเมิน เพื่อให้มีความเหมาะสมกับการใช้งานในระบบอื่น ๆ ต่อไปได้ หรือสามารถนำไปทำการวิจัยต่อยอดเพื่อพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับระบบอื่น ๆ ตามความเหมาะสมต่อไป

บรรณานุกรม

ปริญญา หอมเอนก. 2560. Understanding CsP-MICS NexusFour Model and Cybersecurity Resilience Framework. ACIS Cyber LAB Team.

เอกฉัตร บ่ายคล้อย และประสงค์ ปราณีตพลกรัง. 2560. ความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศในระบบประมวลผล แบบคลาวด์. การประชุมวิชาการระดับชาติ และนานาชาติ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี.

Alexander Kott., and Igor Linkov. 2018. Cyber Resilience of Systems and Networks (Risk, Systems and Decisions). Springer.

Deborah J. Bodeau., and Richard Graubart. 2017. Cyber Resiliency Design Principles. MITRE TECHNICAL REPORT.

Deborah J. Bodeau., and Richard Graubar. 2017. Cyber Resiliency Engineering Framework. MITRE TECHNICAL REPORT.

Deborah J. Bodeau., and Richard Graubart. 2016. Cyber Resilience Metrics Key Observations. THE MITRE CORPORATION.

Del Alfred. (2014). CISO Leadership: Cyber Security Top Cop. D Alfred.

Francesco Flammini. 2018. Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction (Advanced Sciences and Technologies for Security Applications). Springer.

Gary Warzala. 2015. Cyber Resilience Best Practices. AXELOS Limited.

Gerard Blokdijk. 2018. Cybersecurity Resilience Complete Self-Assessment Guide. The Art of Service.

International Organization for Standardization. 2005. ISO/IEC Standard 27001: Information technology Security techniques Information security management systems Requirements. First Edition.

International Organization for Standardization. 2005. ISO/IEC Standard 27002: Information technology Security techniques Code of practice for information security management. First Edition.

International Organization for Standardization. 2015. ISO/IEC Standard 27017: Information technology Security techniques Code of practice for information security controls based on ISO/IEC 2002 for cloud services.

International Organization for Standardization. 2014. ISO/IEC Standard 27018: Information technology Security techniques Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

National Institute of Standards and Technology. 2010. Framework for Improving Critical Infrastructure Cybersecurity. Draft Version 1.1.

Phillimon Zongo. 2018. The Five Anchors of Cyber Resilience: Why Some Enterprises Are Hacked Into Bankruptcy, While Others Easily Bounce Back. Ciso Advisory.

Phillip King-Wilson. 2012. Cyber Risk & Resilience for (non-I.T.) Managers: Understanding and Managing Internet Connectivity Risks. Quantar SolutionsLimited.

Ray Rothrock. 2018. Digital Resilience: Is Your Company Ready for the Next Cyber Threat?. AMACOM.

Richard A. Caralli., and Julia H. Allen., and Pamela D. Curtis., and David W. White., and Lisa R. Young. 2010. CERT Resilience Management Model Version 1.0. Carnegie Mellon University.

Stuart Shapiro., and Brianna Keys., and Aashish Chhajer., and Zilong Liu., and Daniel Horner. 2016. A FRAMEWORK FOR ASSESSING CYBER RESILIENCE. World Economic Forum.

ภาคผนวก ก

คู่มือการใช้งาน
แอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์

ภาคผนวก ข

แบบการสัมภาษณ์เชิงลึก
ความสามารถ ในการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

ภาคผนวก ค

แบบประเมินตนเอง
การวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์

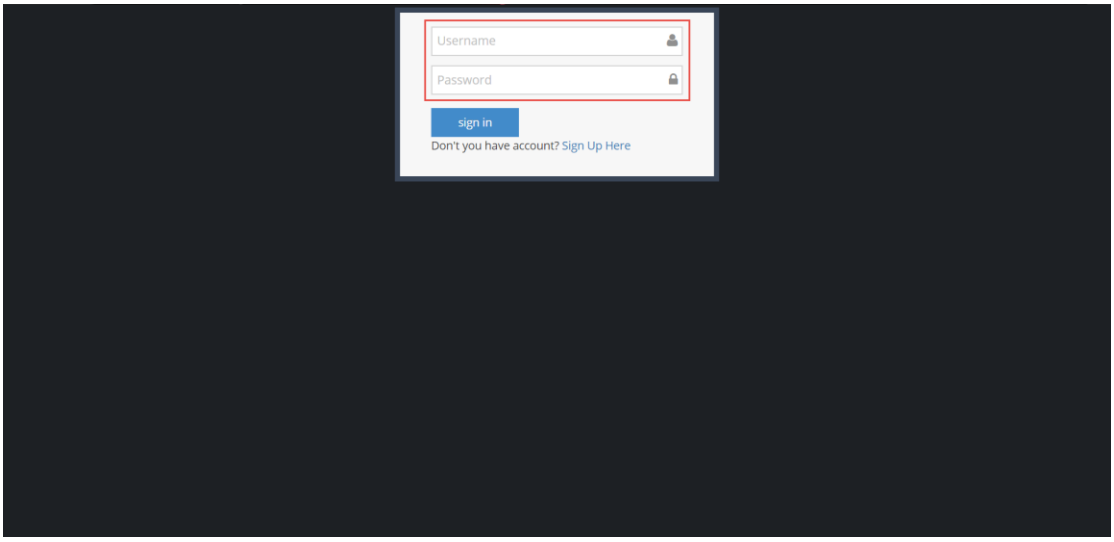
ภาคผนวก ง

ผลงานตีพิมพ์

คู่มือการใช้งาน

แอปพลิเคชันประเมินตนเองสำหรับประเมินการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์

การเข้าสู่ระบบ

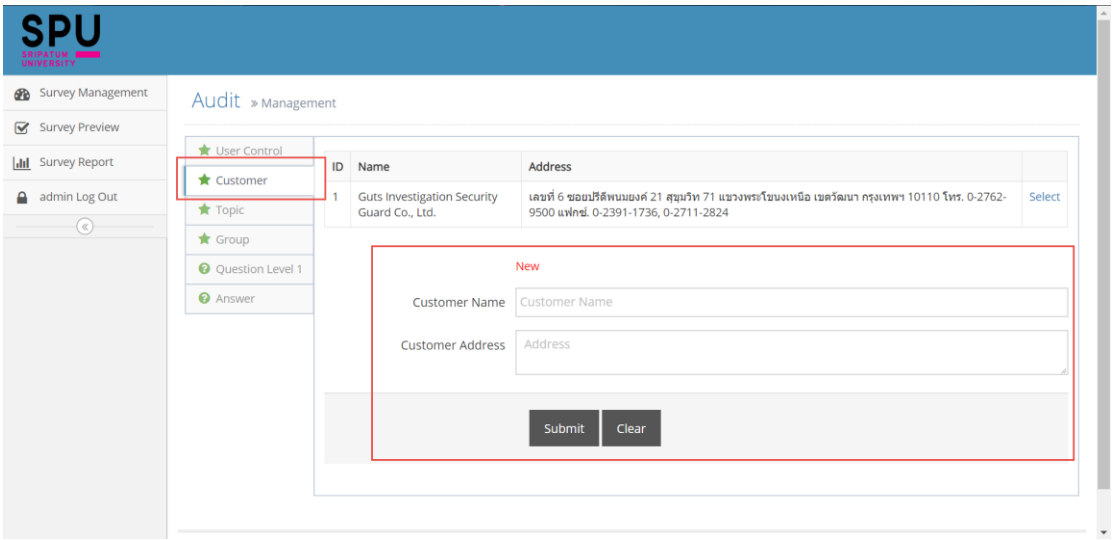


สามารถเข้าสู่ระบบได้จากเว็บบราวเซอร์โดยเข้าไปที่ URL http://staging.epit.co.th

(Username = admin / Password = admin)

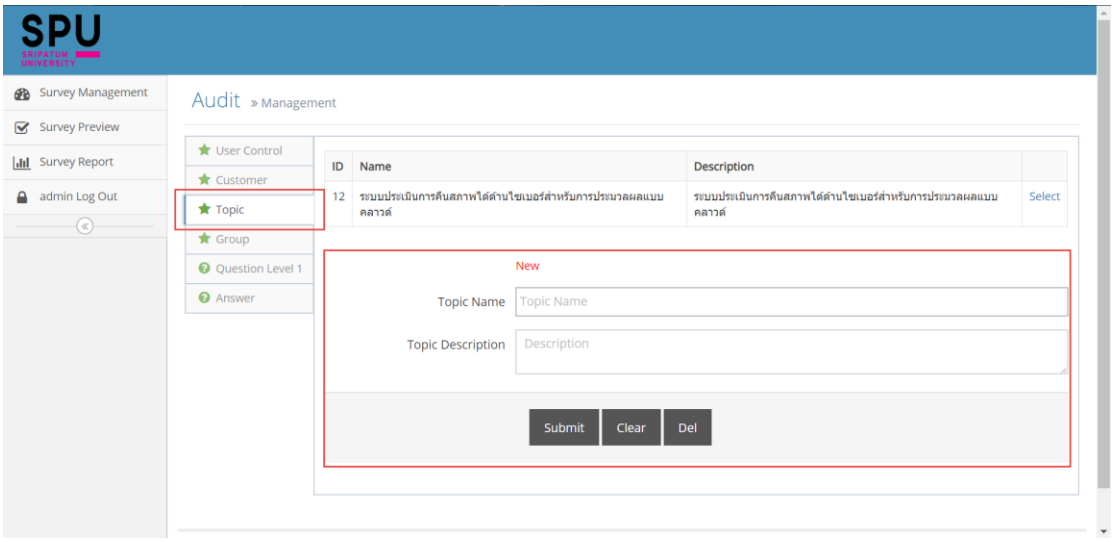
การบริหารจัดการ

การเพิ่มรายชื่อบริษัทหรือองค์กรสำหรับทำการประเมิน



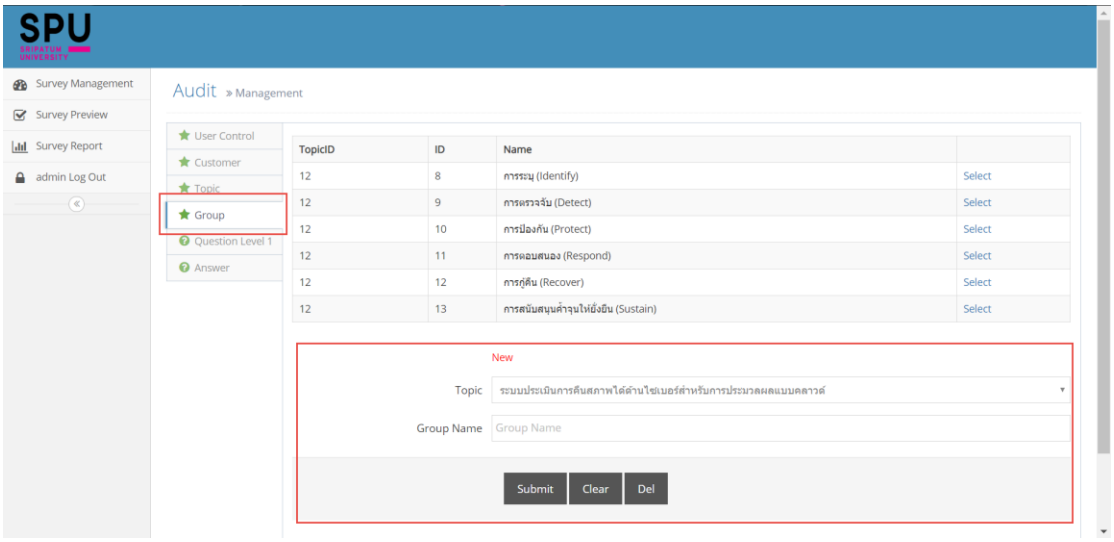
สามารถเพิ่มรายชื่อบริษัทหรือองค์กรสำหรับทำการประเมินโดยเข้าไปที่เมนู Survey Management > Customer สามารถเพิ่มชื่อและที่อยู่ของบริษัทหรือองค์กรและกด Submit เพื่อบันทึก

การเพิ่มชื่อแบบประเมินสำหรับทำการประเมิน



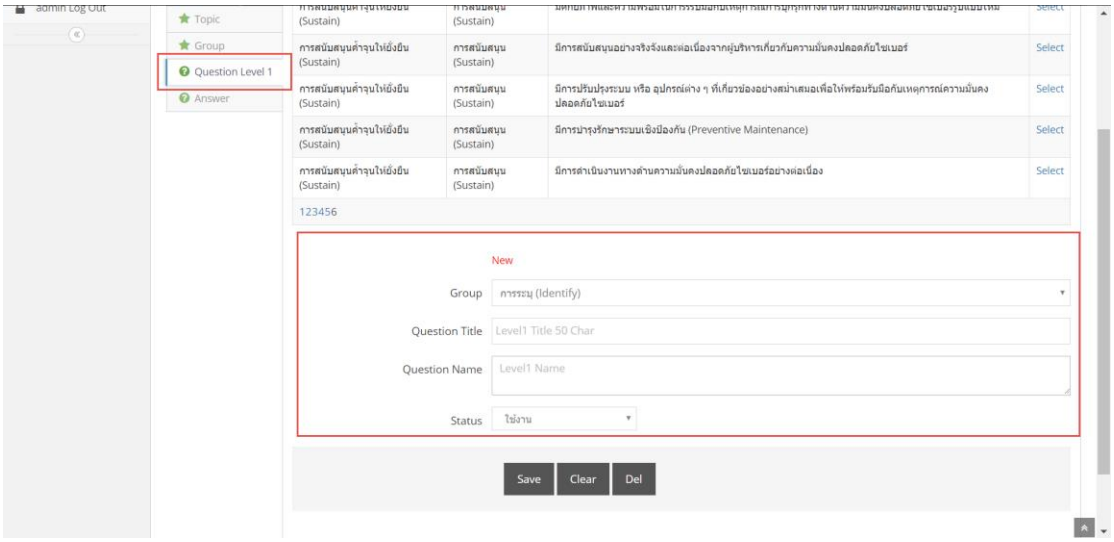
สามารถเพิ่มชื่อแบบประเมินสำหรับทำการประเมินโดยเข้าไปที่เมนู Survey Management > Topic สามารถเพิ่มชื่อแบบประเมินและรายละเอียดและกด Submit เพื่อบันทึก

การเพิ่มชื่อกลุ่มหัวข้อคำถามประเมินสำหรับทำการประเมิน



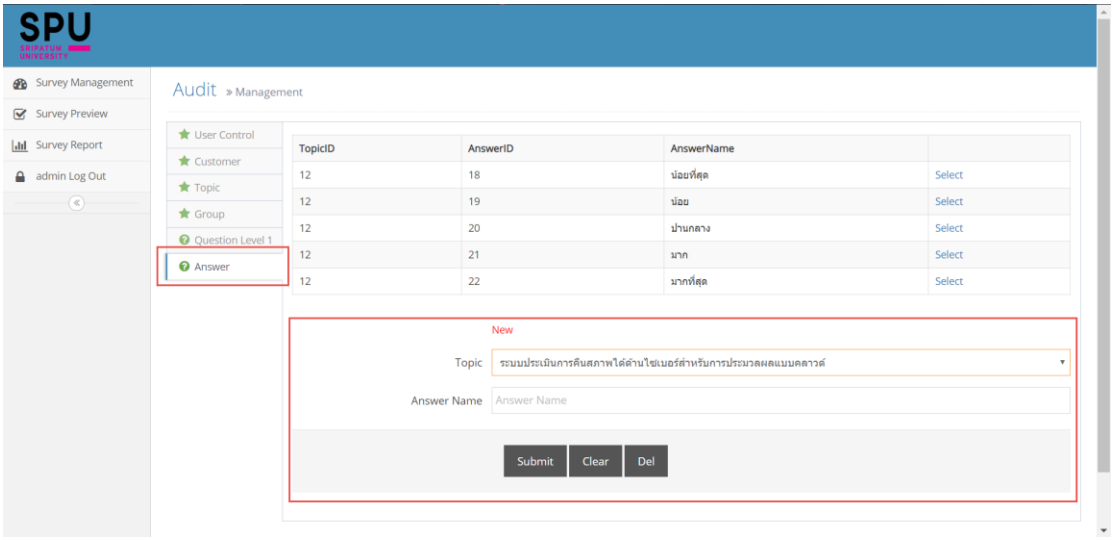
สามารถเพิ่มชื่อกลุ่มหัวข้อคำถามแบบประเมินสำหรับทำการประเมินโดยเข้าไปที่เมนู Survey Management > Group สามารถเลือกชื่อแบบประเมินที่ได้บันทึกไว้ในเมนู Topic และเพิ่มชื่อกลุ่มหัวข้อคำถามแบบประเมินและกด Submit เพื่อบันทึก

การเพิ่มคำถามที่ใช้ประเมินสำหรับทำการประเมิน



สามารถเพิ่มคำถามที่ใช้ประเมินสำหรับทำการประเมินโดยเข้าไปที่เมนู Survey Management > Question Level 1 สามารถเลือกชื่อกลุ่มหัวข้อคำถามที่ได้บันทึกไว้ในเมนู Group และเพิ่มคำถามที่ใช้ประเมินและกด Submit เพื่อบันทึก

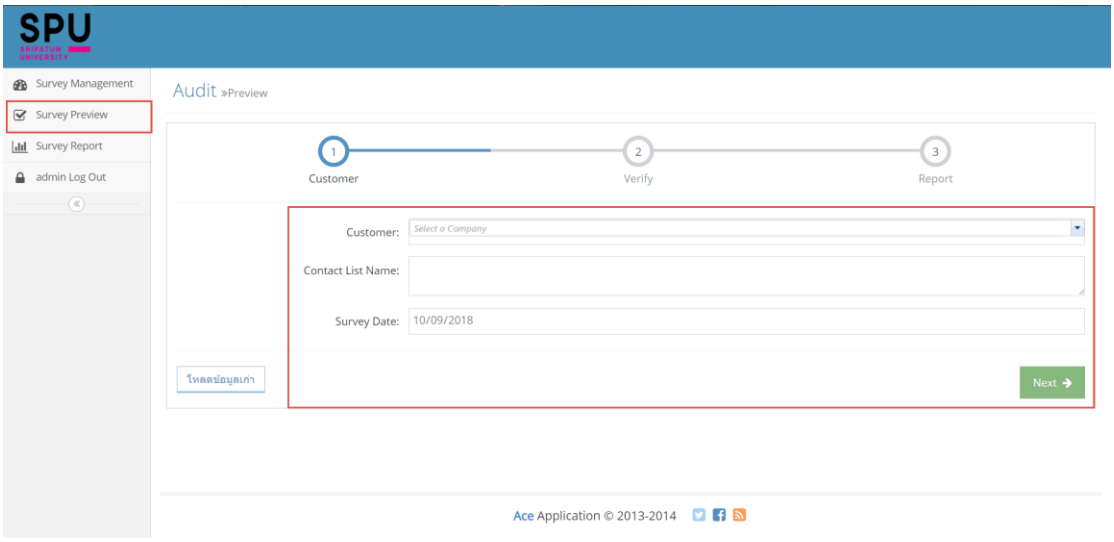
การเพิ่มคำตอบที่ใช้ประเมินสำหรับทำการประเมินตามแบบประเมิน



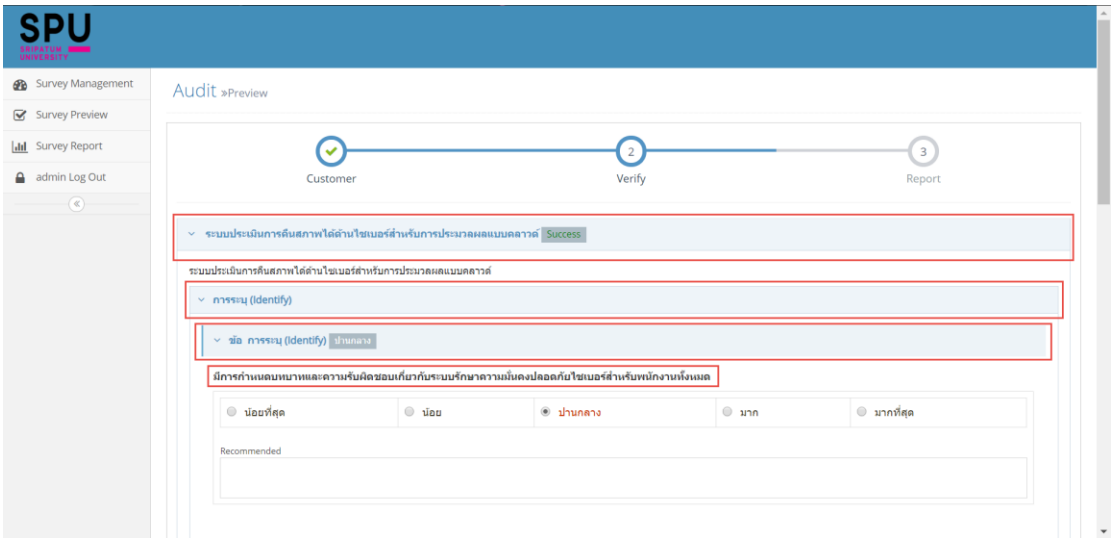
สามารถเพิ่มคำตอบที่ใช้ประเมินสำหรับทำการประเมินโดยเข้าไปที่เมนู Survey Management > Answer สามารถเลือกชื่อแบบประเมินที่ได้บันทึกไว้ในเมนู Topic และเพิ่มคำตอบที่ใช้ประเมินและกด Submit เพื่อบันทึก

การทำการประเมิน

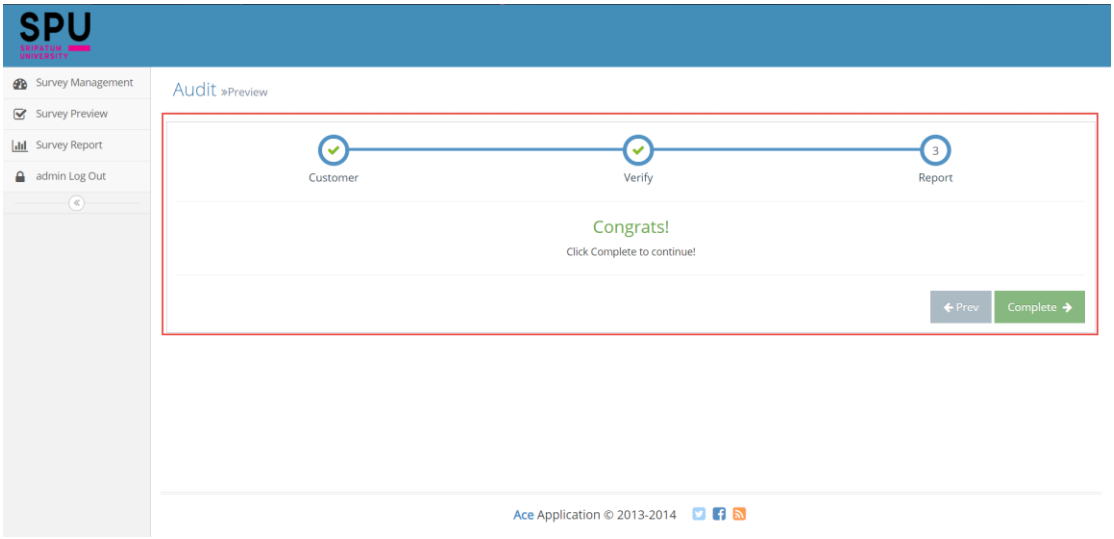
วิธีทำการประเมิน



สามารถทำการประเมินโดยเข้าไปที่เมนู Survey Preview สามารถเลือกชื่อบริษัทหรือองค์กรที่ได้ทำการบันทึกไว้จากนั้นใส่ชื่อผู้ทำการประเมินโดยระบบจะแสดงวันที่ทำการประเมินโดยอัตโนมัติ จากนั้นกด Next เพื่อไปสู่ขั้นตอนต่อไป



ทำการประเมินตามหัวข้อที่สร้างไว้เมื่อครบหมดทุกข้อระบบจะแสดงคำว่า Success หลังจากนั้นกด Next เพื่อไปสู้ขั้นตอนต่อไป



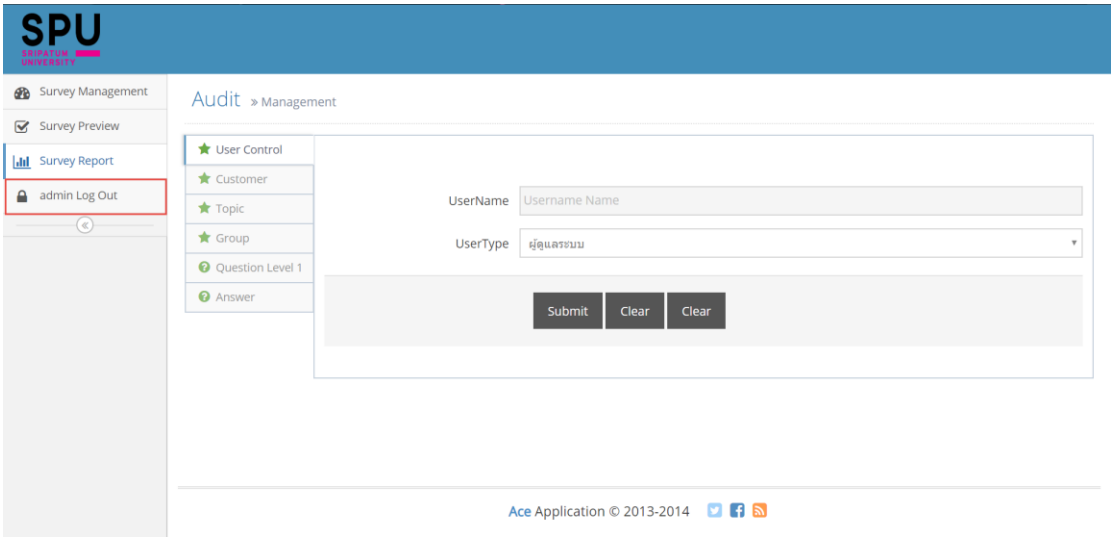
เมื่อทำการประเมินครบทุกขั้นตอนแล้วระบบจะแสดงคำว่า Congrats จากนั้นเลือก Complete เป็นการเสร็จสิ้นการประเมิน

การแสดงผลการประเมิน

เรียกดูรายงานผลการประเมิน

เรียกดูรายงานผลการประเมินให้เลือกที่เมนู Survey Report จากนั้นเลือกชื่อบริษัทหรือองค์กรเพื่อให้ระบบทำการแสดงผลการประเมินที่ได้ทำการประเมินเรียบร้อยแล้ว

การออกจากระบบ



สามารถออกจากระบบการประเมินได้จากเมนู Admin Log Out

ประเด็นการสัมภาษณ์เชิงลึก (In-depth Interview)

เรื่อง "ความสามารถ ในการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์"

ชื่อ ---------- **สกุล** ----------

บริษัท ----------

ตำแหน่ง ----------

วัตถุประสงค์ของการสัมภาษณ์

1. เพื่อแลกเปลี่ยนทัศนคติ แนวคิด ประเด็นปัญหาที่เกี่ยวกับ การคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
2. เพื่อขอคำแนะนำ ข้อเสนอแนะ จากประสบการณ์ในการทำงานของท่าน เพื่อนำมาเป็นแนวคิดในการพัฒนากรอบแนวคิดสำหรับงานวิจัยต่อไป

บทสรุปสำหรับผู้บริหาร

Cloud เป็น 1 ใน Mega Trend IT ที่กำลังเป็นที่นิยมมีทั้งหมด 4 ด้าน ได้แก่ Social (S) , Mobile (M) , Cloud (C) , Big Data (I) หรือ SMCI ซึ่งจากการนำเสนอของ บริษัทการ์ทเนอร์ จะพบว่าส่วนที่เกี่ยวข้องด้านความปลอดภัยไซเบอร์กับ SMCI มีทั้งหมด 2 ปัจจัยคือ 1. Privacy (ความเป็นส่วนตัว), 2. Security (ความปลอดภัย) การจะทำให้ระบบสามารถทำงานได้อย่างถูกต้องและต่อเนื่องจึงจำเป็นที่จะต้องมีมาตรการด้านความมั่นคงปลอดภัยไซเบอร์เข้ามาใช้ในการดำเนินงาน จากการวิจัยของ Information Security Forum (ISF) ระบุว่าระดับของความมั่นคงปลอดภัยไซเบอร์แบ่งได้เป็น 3 ระดับ คือ 1. Information Security, 2. Cybersecurity, 3. Cyber Resilience โดยแบ่งตามประเภทของการรับรู้ทางด้านความปลอดภัยคือ 1. Known CIA คือ การรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อ CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability การรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Information Security , 2. Known non-CIA คือ การรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อระบบอื่นนอกเหนือจาก CIA Triad การรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Cyber security , 3. Unknown คือ การรับมือกับภัยคุกคามที่ไม่เป็นที่รู้จัก หรือไม่เคยพบมาก่อนการรับมือกับภัยคุกคามระดับนี้ได้เรียกว่า Cyber Resilience การ

ที่จะมีความมั่นคงปลอดภัยไซเบอร์ถึงระดับ Cyber Resilience จำเป็นที่จะต้องเริ่มจาก ระดับของ Information Security เสียก่อน

การพัฒนาของเทคโนโลยี มีความรวดเร็วและสามารถเข้าถึงได้ง่ายมากขึ้นทำให้ ปัจจัยต่าง ๆ เอื้อต่อความไม่ปลอดภัยในการใช้งานทั้งในแง่ของ ความลับ ความถูกต้อง และความพร้อมใช้ ยิ่งมีการใช้งานและการเข้าถึงที่ง่ายมากขึ้นเท่าไหร่ ความเสี่ยงทางด้านความปลอดภัยก็ยิ่งมีมากขึ้น ฉนั้นการมีมาตรการความปลอดภัยจึงเป็นสิ่งที่จำเป็น และเข้ามามีบทบาทในการดำเนินงาน ซึ่งความปลอดภัยที่เกิดขึ้นนั้นต้องคำนึงถึงภาพรวมของธุรกิจหรือกิจกรรมต่าง ๆ ที่มีผลกระทบ รวมถึงปัจจัยภายใน และภายนอก ที่อาจจะส่งผลต่อความมั่นคงปลอดภัย การจะพัฒนาระดับความปลอดภัยนั้นผู้บริหารมีความจำเป็นที่จะต้องเข้ามามีส่วนร่วมในการดำเนินงาน รวมถึงผลักดันให้เกิดการยอมรับในองค์กรณ์ ซึ่งจะเห็นได้ว่า กรอบทางด้านการคืนสภาพทางด้านไซเบอร์มีจุดเริ่มมากจาก กรอบการพัฒนาทางด้านความปลอดภัยไซเบอร์ ที่มีการนำมาจัดกลุ่มตามปัจจัยต่าง ๆ ที่มีผลกระทบต่อการดำเนินงาน รามถึงการรับมือทั้งก่อนและหลังเหตุการณ์ความผิดปกติที่เกิดขึ้น มาตรการรับมือต่าง ๆ ที่เกิดขึ้นมีเพียงจุดประสงค์เดียวคือการทำให้ระบบหรือธุรกิจสามารถให้บริการได้อย่างถูกต้องและต่อเนื่อง

นิยามศัพท์

1. **Cloud Computing** หมายถึง ลักษณะการทำงานโดยใช้ทรัพยากรต่างๆ ที่มีอยู่มากมายบนเครือข่ายอินเทอร์เน็ต เช่น พื้นที่เก็บข้อมูล แพลตฟอร์มทางธุรกิจ แอปพลิเคชัน พาณิชย์อิเล็กทรอนิกส์ การตลาดออนไลน์ผู้ใช้งานคอมพิวเตอร์สามารถเลือกใช้งานได้ผ่านผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ที่ให้บริการใดบริการหนึ่งกับผู้ใช้ โดยผู้ให้บริการจะแบ่งปันทรัพยากร ให้กับผู้ต้องการใช้งานนั้น และจ่ายค่าบริการตามการใช้งานจริง
2. **Information Security** หมายถึง ระดับการรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อ CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability
3. **Cyber Security** หมายถึง ระดับการการรับมือกับภัยคุกคามที่เป็นที่รู้จักและส่งผลกระทบต่อระบบอื่นนอกเหนือจาก CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability

4. **Cyber Resilience** หมายถึง ระดับการคืนสภาพได้อย่างรวดเร็วสามารถรับมือกับภัยคุกคามที่ไม่เป็นที่รู้จัก หรือไม่เคยพบมาก่อนสามารถรับมือต่อการเปลี่ยนแปลง รวมทั้งความสามารถในการทนทานต่อการบุกรุก การโจมตี รวมถึงความสามารถในการคืนสภาพของระบบ ไม่ว่าจะเป็นการโจมตีที่เกิดจากปัจจัยภายในหรือภายนอก

แนวคำถามในการสัมภาษณ์

1. ท่านมีความคิดเห็นอย่างไร ต่อปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์ ที่นับวันจะยิ่งทวีความรุนแรงขึ้นนั้น อันจะส่งผลกระทบต่อการดำเนินการในกิจกรรมต่าง ๆ ของระบบการประมวลผลแบบคลาวด์
2. ท่านมีความคิดเห็นอย่างไรต่อความเสี่ยงของภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
3. ท่านมีความคิดเห็นอย่างไร ต่อการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
4. บริษัทของท่าน มีแนวทางหรือแผนการดำเนินงานเกี่ยวกับการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ อย่างไร
5. ในมุมมองของท่านอะไรคือ ปัจจัยสำคัญที่จะมีผลต่อการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
6. ในมุมมองของท่าน ท่านคิดว่าความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ควรมีกรอบหรือรูปแบบอย่างไร
7. ท่านคิดว่า ความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีความสัมพันธ์อย่างไร กับการจัดการทางด้าน บุคลากร (People)
8. ท่านคิดว่า ความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีความสัมพันธ์อย่างไร กับการจัดการทางด้าน กระบวนการ (Process)
9. ท่านคิดว่า ความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีความสัมพันธ์อย่างไร กับการจัดการทางด้าน เทคโนโลยี (Technology)
10. ท่านคิดว่า ความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีความสัมพันธ์อย่างไร กับการจัดการทางด้าน ความลับของข้อมูล (Confidentiality)
11. ท่านคิดว่า ความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีความสัมพันธ์อย่างไร กับการจัดการทางด้าน ความถูกต้องของข้อมูล (Integrity)

12. ท่านคิดว่า ความสามารถในการคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ มีความสัมพันธ์อย่างไร กับการจัดการทางด้าน ความพร้อมใช้ข้อมูล (Availability)
13. ในมุมมองของท่าน สมรรถนะหรือขีดความสามารถขององค์กร ในการสร้างความคืนสภาพได้ทางด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ควรเป็นอย่างไร
14. ในมุมมองของท่าน นโยบายและภาวะผู้นำมีผลอย่างไรต่อ การคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์
15. ท่านมีความคิดเห็นอย่างไร ต่อภาพรวมของ พัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ว่าควรจะมีรูปแบบอย่างไร

แบบประเมินตนเองเรื่อง “การวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์”

<u>คำชี้แจง</u>

แบบประเมินตนเองนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นของท่านเกี่ยวกับความสามารถในการฟลิกฟื้นหรือฟื้นตัวหรือการคืนสภาพได้ (Resilience) สำหรับระบบการประมวลผลแบบคลาวด์ ผู้วิจัยใคร่ขอความร่วมมือในการตอบแบบสอบถาม โดยขอความกรุณาท่านให้ข้อมูลหรือแสดงความคิดเห็นที่ตรงกับความเป็นจริงมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาวัยทางวิชาการเท่านั้น ผู้วิจัย ขอรับรองว่าข้อมูลที่ได้จากแบบสอบถามจะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายกับท่านหรือผู้ที่เกี่ยวข้องแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถาม

ส่วนที่ 2 ความคิดเห็นเกี่ยวกับการคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์

ส่วนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

การแปลผลระดับความคิดเห็น แบ่งเป็น 5 ระดับ ดังต่อไปนี้

5	หมายถึง	ระดับมากที่สุด
4	หมายถึง	ระดับมาก
3	หมายถึง	ระดับปานกลาง
2	หมายถึง	ระดับน้อย
1	หมายถึง	ระดับน้อยที่สุด

นิยามศัพท์ที่เกี่ยวข้อง

1. **การประมวลผลแบบคลาวด์ (Cloud Computing)** หมายถึง รูปแบบหนึ่งของการประมวลผลโดยใช้ทรัพยากรร่วมกันผ่านเครือข่ายตามความต้องการได้อย่างสะดวกรวดเร็วจากทุกแห่งหน ทั้งนี้ ผู้ใช้ไม่ต้องบริหารจัดการทรัพยากรเอง ตัวอย่างทรัพยากร เช่น เครือข่าย เครื่องแม่ข่าย หน่วยเก็บ ซอฟต์แวร์ ประยุกต์และบริการ

2. **การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)** หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม

3. **การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience)** ระดับการรับมือกับภัยคุกคามที่ไม่เป็นที่รู้จัก หรือไม่เคยพบมาก่อนสามารถรับมือต่อการเปลี่ยนแปลง รวมทั้งความสามารถในการทนทานต่อการบุกรุก การโจมตี รวมถึงความสามารถในการคืนสภาพของระบบ ไม่ว่าจะเป็นการโจมตีที่เกิดจากปัจจัยภายในหรือภายนอก

ผู้วิจัย

นายจิราพัชร์ พันธุ์ถาวรชัย อีเมล : bing.jirapat@gmail.com โทรศัพท์ 09-7083-3336

นักศึกษา หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ส่วนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบประเมินตนเอง

โปรดทำเครื่องหมาย ✓ ในช่อง ☐ ที่ตรงกับข้อมูลของท่าน เพียงช่องเดียว

1. เพศ ☐ 1) ชาย ☐ 2) หญิง
2. อายุ ☐ 1) 20-30 ปี ☐ 2) 31-40 ปี
   ☐ 3) 41-50 ปี ☐ 4) 51-60 ปี
3. ตำแหน่ง ☐ 1) เจ้าหน้าที่ระดับปฏิบัติการ ☐ 2) หัวหน้าฝ่าย
   ☐ 3) หัวหน้าแผนก ☐ 4) ผู้อำนวยการ
4. ระยะเวลาที่ปฏิบัติงาน ☐ 1) น้อยกว่า 1 ปี ☐ 2) 1-5 ปี
   ☐ 3) 5-10 ปี ☐ 3) มากกว่า 10 ปี
5. ท่านเคยประสบภัยคุกคามทางไซเบอร์หรือไม่ ☐ 1) เคย ☐ 2) ไม่เคย

ส่วนที่ 2 ระดับความคิดเห็นของผู้ให้บริการแบบคลาวด์สำหรับวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์

โปรดทำเครื่องหมาย ✓ ในช่อง ที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด

หัวข้อวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์	ระดับความเห็น				
	5	4	3	2	1
1. การระบุ (Identify)					
1.1 มีการกำหนดบทบาทและความรับผิดชอบเกี่ยวกับระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงานทั้งหมด					
1.2 มีการบ่งบอกหรือกำหนดความต้องการเกี่ยวกับระบบรักษาความมั่นคงปลอดภัยไซเบอร์จากการใช้บริการภายนอก (Outsource)					
1.3 มีการระบุผู้ที่เข้ามาใช้งานระบบ					
1.4 มีกระบวนการประเมินความเสี่ยงทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมกับระบบงานสำคัญยิ่งยวด (Critical Systems)					

หัวข้อวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์	ระดับความเห็น				
	5	4	3	2	1
1.5 มีกระบวนการในการตรวจสอบเพื่อป้องกันการเปลี่ยนแปลงแก้ไขอุปกรณ์ โปรแกรม และระบบงานโดยไม่ได้รับอนุญาต					
1.6 มีการจัดระดับความสำคัญของระบบต่าง ๆ ที่ทำงานร่วมกัน					
1.7 มีเครื่องมือหรืออุปกรณ์ที่สามารถระบบเฝ้าสังเกต (Monitor) เหตุการณ์ที่เกิดขึ้นกับระบบ					
1.8 มีเครื่องมือหรืออุปกรณ์ที่สามารถระบุช่องโหว่ของระบบ (Vulnerability Scan)					
1.9 มีเครื่องมือหรืออุปกรณ์ในการทดสอบความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบ (Penetration Test)					
1.10 มีการกำหนดให้ประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานซอฟต์แวร์และฮาร์ดแวร์ที่หยุดสนับสนุน (End of Support) แล้ว					
2. การตรวจจับ (Detect)					
2.1 มีกระบวนการในการประเมินความเหมาะสมของของคุณสมบัติและศักยภาพของบุคลากรกับหน้าที่ความรับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง					
2.2 มีกระบวนการตรวจสอบผลการปฏิบัติงานการใช้บริการภายนอก (Outsource)					
2.3 มีกระบวนการตรวจสอบประวัติและพฤติกรรมของบุคลากรตามความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบอย่างต่อเนื่อง					
2.4 มีกระบวนการตรวจหาการทำงานที่ผิดปกติของอุปกรณ์ที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัยไซเบอร์					
2.5 มีกระบวนการตรวจสอบเฝ้าสังเกตเครือข่ายและอุปกรณ์ที่เกี่ยวข้อง					
2.6 มีกระบวนการปรับปรุงการตรวจสอบเฝ้าสังเกตเครือข่ายและอุปกรณ์ที่เกี่ยวข้อง					
2.7 มีเครื่องมือที่ช่วยในการตรวจสอบโค้ดเจตนาร้าย (Malicious Code)					
2.8 มีอุปกรณ์หรือโปรแกรมที่ช่วยในการตรวจหาการโจมตีทางระบบเครือข่าย เช่น ไฟร์วอลล์ (Firewall)					
2.9 มีการใช้งานโปรแกรมตรวจสอบและป้องกันไวรัส (Anti Virus)					

หัวข้อวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์	ระดับความเห็น				
	5	4	3	2	1
3. การป้องกัน (Protect)					
3.1 มีกระบวนการป้องกันความผิดพลาดที่เกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร					
3.2 มีกระบวนการป้องกันความผิดพลาดที่เกี่ยวข้องกับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์จากการใช้บริการภายนอก (Outsource)					
3.3 มีการฝึกอบรมเพื่อเพิ่มศักยภาพความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรที่มีส่วนเกี่ยวข้องอย่างต่อเนื่อง					
3.4 มีการกำหนดกระบวนการในการรับมือกับเหตุการณ์การบุกรุกด้านความมั่นคงปลอดภัยไซเบอร์ไว้อย่างชัดเจน					
3.5 มีการทดสอบเพื่อเตรียมความพร้อมในการรับมือกับเหตุการณ์การบุกรุกด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง					
3.6 มีการรับข่าวสารจากภายนอกเพื่อเพิ่มระดับการรับรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง					
3.7 มีการใช้งานซอฟต์แวร์หรือฮาร์ดแวร์เพื่อช่วยในการควบคุมอุปกรณ์ที่เชื่อมต่อกับระบบที่ใช้งานอยู่					
3.8 มีการใช้งานซอฟต์แวร์หรือฮาร์ดแวร์เพื่ออำนวยความสะดวกให้ผู้ใช้งานที่เชื่อมต่อกับระบบ					
3.9 มีการใช้งานระบบป้องกันการบุกรุก หรือระบบการตรวจหาการบุกรุก					
3.10 มีการตรวจสอบความถูกต้องของการตั้งค่าอุปกรณ์ที่ใช้งาน					
4. การตอบสนอง (Respond)					
4.1 มีการกำหนดหน้าที่ความรับผิดชอบสำหรับบุคลากรในการตอบสนองต่อเหตุการณ์การบุกรุกด้านความมั่นคงปลอดภัยไซเบอร์ไว้อย่างชัดเจน					
4.2 มีการกำหนดหน้าที่ความรับผิดชอบสำหรับการใช้บริการภายนอก (Outsource) ในการตอบสนองต่อเหตุการณ์การบุกรุกด้านความมั่นคงปลอดภัยไซเบอร์ไว้อย่างชัดเจน					

หัวข้อวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์	ระดับความเห็น				
	5	4	3	2	1
4.3 มีกระบวนการส่งต่อหน้าที่ความรับผิดชอบของบุคลากรในการตอบสนองด้านความมั่นคงปลอดภัยไซเบอร์					
4.4 มีการใช้ข้อมูลจากภายนอกร่วมกับการวางแผนการตอบสนองด้านความมั่นคงปลอดภัยไซเบอร์					
4.5 มีกระบวนการทำงานเพื่อแก้ปัญหาช่องโหว่ในระบบ					
4.6 มีการนำเหตุการณ์ที่เคยเกิดขึ้นมาร่วมในการวางแผนปรับปรุงแผนการตอบสนองด้านความมั่นคงปลอดภัยไซเบอร์					
4.7 มีระบบการตอบสนองต่อเหตุการณ์ (Incident Response) เมื่อผู้ที่มีส่วนเกี่ยวข้องถูกโจมตีหรือคุกคามทางไซเบอร์					
4.8 มีการรับประกันการใช้งานของอุปกรณ์เครือข่ายเมื่อเกิดการชำรุดหรือไม่ทำงานให้สามารถทำงานได้ภายในระยะเวลาที่กำหนด					
4.9 มีการปรับปรุงแผนและแนวทางปฏิบัติการตอบสนองการบุกรุกอย่างยืดหยุ่น					
5. การกู้คืน (Recover)					
5.1 มีแนวทางและแผนในการสรรหา ดูแลรักษา และจัดหาทดแทนพนักงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์					
5.2 มีการติดต่อใช้บริการภายนอก (Outsource) เพื่อแก้ไขปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่สามารถแก้ไขได้					
5.3 มีการกำหนดนโยบายและวางแผนในการกู้คืนระบบเพื่อให้ระบบสามารถทำงานต่อไปได้อย่างปกติ					
5.4 มีการนำเหตุการณ์ที่เคยเกิดขึ้นมาร่วมในการวางแผนปรับปรุงการปฏิบัติในการกู้คืน					
5.5 แผนการกู้คืนที่กำหนดไว้สามารถดำเนินการได้ในระหว่างหรือหลังการเกิดเหตุการณ์ผิดปกติ					
5.6 มีแนวทางการประเมินสมรรถนะบุคลากรที่ทำหน้าที่รับผิดชอบเกี่ยวกับแผนการกู้คืน					

หัวข้อวิเคราะห์การคืนสภาพได้สำหรับระบบการประมวลผลแบบคลาวด์	ระดับความเห็น				
	5	4	3	2	1
5.7 มีระบบสำรองที่สามารถทำงานคู่ขนานหรือทดแทนระบบเดิมได้ทันที					
5.8 มีการใช้งานระบบสำรองข้อมูล (Backup) จากภายในและภายนอกหน่วยงาน					
6. การสนับสนุน (Sustain)					
6.1 มีการสร้างความตระหนักรู้และความเข้าใจแก่บุคลากรที่เกี่ยวข้องถึงผลกระทบทางด้านความมั่นคงปลอดภัยไซเบอร์					
6.2 มีการสร้างความตระหนักรู้และความเข้าใจแก่บุคลากรถึงความสำคัญในบทบาทหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์					
6.3 มีการเพิ่มทักษะและความสามารถทางด้านที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แก่บุคลากร					
6.4 มีการกำหนดนโยบายและมาตรฐานการปฏิบัติเพื่อรักษาระดับของความมั่นคงปลอดภัยไซเบอร์					
6.5 มีศักยภาพและความพร้อมในการรับมือกับเหตุการณ์การบุกรุกทางด้านความมั่นคงปลอดภัยไซเบอร์รูปแบบใหม่					
6.6 มีการสนับสนุนอย่างจริงจังและต่อเนื่องจากผู้บริหารเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์					
6.7 มีการปรับปรุงระบบ หรือ อุปกรณ์ต่าง ๆ ที่เกี่ยวข้องอย่างสม่ำเสมอเพื่อให้พร้อมรับมือกับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์					
6.8 มีการบำรุงรักษาระบบเชิงป้องกัน (Preventive Maintenance)					
6.9 มีการดำเนินงานทางด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง					

ส่วนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

.....

.....

.....

.....

ผู้วิจัย ขอกราบขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม

[1] Jirapat Phantawornchai, Ekkachat Baikloy and Prasong Praneetpolgrang, **"Cybersecurity Resilience Framework Consideration of Cloud Computing,"** The 6th International Conference on Robotics, Informatics and Intelligent Control Technology, 4 – 6 September 2018, Asia Hotel Bangkok, Thailand.

Abstract

Presently, the using of cloud computing is gaining popularity and widespread use. Increasing the Cybersecurity measures is more needed. This research aims to develop the Cybersecurity Resilience Framework for Cloud Computing by using NIST Core Cybersecurity Framework. The researchers conducted the semi structured interviews and group discussion with the cyber security experts. The researchers found the key of the Cybersecurity Resilience Framework Consideration of Cloud Computing as regarding 1) Data 2) Awareness and understanding of business, and 3) Flexibility of systems that rely on people, processes and technology. In addition, the research results of Cybersecurity Resilience Framework Consideration of Cloud Computing are also used in the data resilience analysis for enterprise cloud computing. According to the assessment of cybersecurity resilience in cloud computing by cloud service providers. It was found the readiness is high level.

[2] จิราพัชร์ พันธุ์ถาวรชัย, เอกฉัตร บ่ายคล้อย และ ประสงค์ ปราณีตพลกรัง, **“การพัฒนากรอบการคืนสภาพได้ทางไซเบอร์สำหรับการประมวลผลแบบคลาวด์,”** วารสารเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ฉบับที่ xx.

บทคัดย่อ

ระบบการประมวลผลแบบคลาวด์ กำลังได้รับความนิยมมากในปัจจุบัน เนื่องจากการใช้งานที่สะดวกและสามารถใช้งานได้จากทุกที่ องค์กรส่วนใหญ่เริ่มเปลี่ยนไปใช้งานระบบการประมวลผลแบบคลาวด์มากขึ้น ด้วยเหตุนี้ จึงจำเป็นต้องเพิ่มมาตรการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มากขึ้น งานวิจัยนี้มีจุดประสงค์เพื่อพัฒนากรอบการคืนสภาพได้ทางไซเบอร์สำหรับการประมวลผลแบบคลาวด์ และจัดทำแบบประเมินพร้อมกับแอปพลิเคชันในการประเมินระดับการคืนสภาพได้ทางไซเบอร์ของระบบการประมวลผลแบบคลาวด์ ผู้วิจัยได้ใช้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา ประกอบกับการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญ และการสนทนากลุ่ม กับผู้ทรงคุณวุฒิ

ผลการวิจัย พบว่าหลักการสำคัญของการคืนสภาพได้ทางไซเบอร์ของระบบการประมวลผลแบบคลาวด์คือ 1) ความถูกต้องของข้อมูล 2) ความพร้อมในการคืนสภาพของระบบ 3) ความตระหนักถึงหน้าที่ความรับผิดชอบของบุคลากร ผู้วิจัยยังได้พัฒนากรอบการคืนสภาพได้ทางไซเบอร์สำหรับการประมวลผลแบบคลาวด์พร้อมทั้งจัดทำแบบประเมินระดับการคืนสภาพได้ทางไซเบอร์ของระบบการประมวลผลแบบคลาวด์ ซึ่งจากการประเมินผู้ให้บริการแบบคลาวด์ในประเทศไทยพบว่ามีการคืนสภาพได้ทางไซเบอร์อยู่ในระดับมาก

ประวัติผู้วิจัย

ชื่อ – สกุล นาย จิราพัชร์ พันธุ์ถาวรชัย

วันเดือนปีเกิด 11 ธันวาคม พ.ศ.2531

ประวัติการศึกษา Bachelor's Degree of Business computer. 2011, มหาวิทยาลัยราชพฤกษ์

อาชีพ พนักงานบริษัทเอกชน

ตำแหน่ง Senior System Engineer

ประสบการณ์

1. ติดตั้งและบำรุงรักษาระบบเครื่อค่ายเน็ตเวิร์คให้กับลูกค้า เช่น Load balance, Firewall, Network Switch, WiFi Hotspot, VDO Streaming, VoIP
2. Implement Storage,Server,OS(VMware),Backup : Thung hua sing printing
3. Implement Access point 100 Branch : B-Quik
4. Implement Storage, Server, OS(VMware),Backup : S.Napa
5. Implement Server, OS(VMware) : Starsmicro
6. Implement Server, Storage, Backup : Seavalue
7. Implement Server, OS(Hyper-v), Backup, Firewall : Blackmores
8. Implement Server, Storage, Backup : European Snack Food
9. Implement Server, Storage, Backup, Firewall : Guts investigation
10. Implement Server, Storage, OS (VMware) : Fragrant Property Group
11. Implement Server, Storage, OS (VMware, Windows),Backup : V-E
12. Implement Firewall : Cloud-Sec Asia
13. Implement Network & Firewall : Bangkok Air Catering.

ผลงานวิชาการที่ได้รับการตีพิมพ์

[1] Jirapat Phantawornchai, Ekkachat Baikloy and Prasong Praneetpolgrang, **"Cybersecurity Resilience Framework Consideration of Cloud Computing,"** The 6th International Conference on Robotics, Informatics and Intelligent Control Technology, 4 – 6 September 2018, Asia Hotel Bangkok, Thailand.

[2] จิราพัชร์ พันธุ์ถาวรชัย, เอกฉัตร บ่ายคล้อย และ ประสงค์ ปราณีตพลกรัง, **"การพัฒนากรอบการคืนสภาพได้ทางไซเบอร์สำหรับการประมวลผลแบบคลาวด์,"** วารสารเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ฉบับที่ xx.